STANDARD FUNCTIONAL SPECIFICATIONS FOR LAW ENFORCEMENT RECORDS MANAGEMENT SYSTEMS VERSION IV

Prepared by the Joint RMS Standards Task Force

ACKNOWLEDGEMENTS

Following a great deal of commitment and effort by many contributors, the Law Enforcement Records Management Systems (RMS) Standard 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 2024-2025 RMS Task Force included law enforcement technology practitioners, subject matter experts, and industry representatives from across the country and Canada. Known as the RMS Task Force, the following individuals have generously contributed their time and expertise to the latest revision of this essential document.

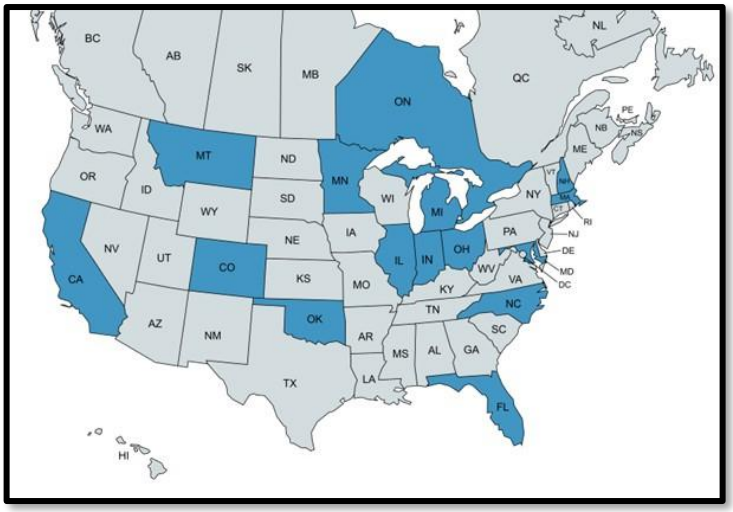
Catherine A. Miller, Chair
Program Manager, National Capital Region
Law Enforcement Information Exchange (NCR-LInX)
Montgomery County (MD) Police Department

Todd Thompson, Co-Chair
Sr Vice President, Strategic Development
Harris Computer— Frontline Public Safety Group

Melissa J. Winesburg, PhD, Co-Chair
Director of Programs, IJIS Institute

TASK FORCE MEMBERS

Lt. Jon Albee, McLean County (IL) Sheriff's Office
Capt. David Baisden, Oklahoma Co. (OK) Sheriff's Office
John Beardsley, Greenville (NC) Police Department
Sgt. Corey Berfield, Indiana State Police Department
Anna Berger, Montgomery County (MD) Police Dept.
Alison Brooks, International Data Corporation (IDC)
Ed Claughton, PRI Management Group
Lori Cox, Mark43
Darin Dillard, Caliber Public Safety
Anne Dormady, Montana Div. of Criminal Investigations
Boris Duran, Santa Ana (CA) Police Department
Beth Hart, Baltimore City (MD) Police Department
Sgt. John Peterson, Taunton (MA) Police Department
Deputy Chief Scott Roach, Powell (OH) Police Dept.
Donnie Sawin, Wilton (NH) Police Department
Tanya Stauffer, Innova Solutions
Subashi Stendahl, Innova Solutions
Amanda Stierman, Tyler Technologies
Patti Zafke, Full Circle Training Solutions



Geographical Representation of the 2024-2025 RMS Task Force

We would also like to recognize the additional practitioners and industry partners who responded to the call to review and provide feedback on this updated version of the publication. Their expertise and insights have been instrumental in strengthening the document, making it more comprehensive and valuable.

Crystal Combs, City of Charlotte, NC
Alexia Cooper, Bureau of Justice Statistics (BJS)
Samantha Gwinn, The Policing Lab
Bonnie Locke, Nlets Consultant
Joe Mandala, Mandala ITC
Debra Piehl, IADLEST
Catherine Watson, AT&T Public Sector & FirstNet
Chris Weatherly, FBI CJIS Division

PUBLISHED MAY 2025

SPECIAL RECOGNITION

The 2024–2025 version of the RMS Standard Functional Specifications document reflects a remarkable collaboration between a new group of justice practitioners and industry partners. These individuals generously dedicated their time and expertise to updating and providing a comprehensive document review. The RMS Task Force would like to recognize Chief Michael Miller, Colleyville Police, and Bonnie Locke for working with their respective sections and committees to identify practitioners who were willing to commit time to work on updating this version of the document.

Additionally, we appreciate the leadership provided by RMS Task Force Chair Catherine Miller and Co-Chairs Todd Thompson and Melissa Winesburg, who were instrumental to the success of this effort. They pulled together this new group of practitioners and industry partners and spent many hours meeting with the teams, organizing comments and edits received to finalize this version of the document. Further, we appreciate the support of the IJIS Institute for their contribution to underwrite the publication of this report. The IJIS team, including Director of Programs Melissa Winesburg, Communications Specialist Alex McAdoo, and B.J. Rentfrow, Studio26, spent many hours managing the comments provided by the RMS Task Force teams, updating graphics, editing sections, and helping to facilitate working group sessions.

Finally, the efforts of the task force leaders and the IJIS Institute staff in producing the final report contributed significantly to the realization of this valuable publication.

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

EXECUTIVE SUMMARY

HISTORY

The IACP CJIS Committee and the IJIS Institute Law Enforcement Advisory Committee (LEAC) have continued their collaborative efforts to update the Law Enforcement Records Management System (RMS) Standard Functional Specifications Document, ensuring it remains relevant and responsive to evolving law enforcement needs. The first task force was formed in the spring of 2019 and spent many months reviewing the foundational RMS functional specifications developed by the Law Enforcement Information Technology Standards Council (LEITSC). Those original specifications were first released as Version I in June 2006, with an updated Version II completed in 2009. Both of these versions received support from numerous federal government and national organizations. Following the disbandment of LEITSC, the document remained unchanged until Version III was published in April 2021 to address emerging technologies and operational requirements.

Recognizing the rapid pace of change in law enforcement technology and practices, the Task Force and partner organizations have adopted a strategy of incremental updates. In 2024, new Task Force members were onboarded and began collaborative efforts to revise areas previously identified for improvement. By publishing this 2025 edition and committing to a regular review cycle, we strive to maintain the RMS Specifications Document as a living resource. The Task Force will continue updating the specifications to incorporate new technologies, address emerging challenges, and reflect the most current best practices in law enforcement. This approach ensures agencies have access to modern, relevant, and robust guidelines for effective RMS implementation and management.

PURPOSE

This document provides law enforcement agencies with a comprehensive guide to understanding and evaluating their RMS needs. Since the last major update in 2009, advancements in technology, changes in operational practices, and evolving data-sharing requirements have highlighted the need for updated functional specifications. In 2019, the IACP CJIS Committee and the IJIS Law Enforcement Advisory Committee (LEAC) recognized the importance of revising these specifications to support agencies during the request for proposal (RFP) and procurement processes. The 2025 edition builds upon previous versions, introducing modifications to align with current law enforcement needs, including cloud-hosted environments, enhanced data interoperability, and compatibility with systems such as the National Incident-Based Reporting System (NIBRS) and National Data Exchange (N-DEx).

This document was developed with the following goals:

- Serve as a foundational resource for agencies developing RMS RFPs.
- Serve as a resource for individuals new to law enforcement and/or RMS.
- Streamline the implementation and maintenance of RMS solutions to reduce costs and improve efficiency.
- Promote information sharing, interoperability, and the adoption of best practices.

Recognizing that an RMS covers the entire lifespan of records—from initial generation to final disposition—this document reflects updates that address both existing business functions and new capabilities driven by emerging technologies. While this document is not intended to serve as a comprehensive requirements specification, it offers suggested guidelines to help agencies identify and define their specific RMS needs. It highlights key considerations based on established standards, recent technological developments, and current policies at the time of publication. Agencies are encouraged to tailor these specifications to their unique operational requirements when assessing, evaluating, procuring, or upgrading RMS solutions. Agencies may also benefit from other resources such as peer networking platforms, procurement guides, solution comparison tools and directories of solution providers. For additional details, including direct links and descriptions of these resources, see the Helpful Resources section at the end of this document.

These specifications are intended to be used in conjunction with other technical standards, such as the National Information Exchange Model (NIEMOpen)[i], The FBI CJIS Security Policy, and international law enforcement technical standards like the United Kingdom's Management of Police Information (MoPI) Standards. This approach helps streamline the information-sharing process, fosters interoperability, and ensures RMS solutions are adaptable to local and global law enforcement environments.

INTRODUCTION

A Records Management System (RMS) is an agency-wide solution designed to manage, store, retrieve, retain, and view records related to law enforcement operations. It serves as the primary system of record for a wide range of policing activities, including incident and accident reports, arrests, citations, warrants, case management, property and evidence tracking, and other operational records.

The 2025 edition of the Standard Functional Specifications for Law Enforcement RMS builds upon previous versions to include essential updates reflecting technological advancements, evolving data-sharing requirements, and changes in law enforcement policies and practices. This edition introduces new features and has been reorganized to address emerging challenges, ensuring law enforcement agencies have the most current and relevant guidance for effective RMS implementation.

In response to law enforcement's growing demands, this version emphasizes the integration of modern technologies, such as cloud-hosted environments, artificial intelligence (AI), and enhanced data security. Cloud technology offers scalability, flexibility, and improved collaboration across jurisdictions, while AI can support smarter decision-making through data analysis and predictive insights. Furthermore, as law enforcement practices and policies evolve, the RMS must be adaptable to emerging standards and regulations, ensuring compliance with national and international frameworks.

An RMS in public safety manages the entire records lifecycle, from initial creation to final disposition. It should enable single-entry data input, reducing redundancy and improving efficiency while also supporting multiple reporting mechanisms to streamline operations. An effective RMS is designed to handle records directly related to public safety activities, such as incident reports, arrests, citations, case management, accident reports, warrants, property and evidence management, and field contacts. While typical RMS solutions do not cover general business functions like budgeting, payroll, or human resources, they may include operational records such as duty rosters or vehicle fleet maintenance, depending on the agency's specific needs.

This updated edition also highlights the importance of data interoperability, compatibility with national systems like the National Data Exchange (N-DEx) and National Incident-Based Reporting System (NIBRS), and compliance with evolving security and privacy standards. All chapters in this document are organized into two categories: core modules and optional modules. Core modules represent foundational RMS functions necessary for most law enforcement agencies to manage day-to-day operations such as incident reporting, arrest processing, and case management. Optional modules address more specialized functionality that may be applicable based on an agency's size, jurisdiction, or operational responsibilities such as equipment tracking, civil process, or permitting.

This structure is intended to help agencies prioritize system requirements based on their unique operational scope while providing flexibility to adopt additional capabilities as needed. While modules are presented as core or optional, each agency should ultimately determine which functions are essential based on its size, responsibilities, and jurisdictional needs.

Foundational Framework

- Chapter 1: General Recommendations
- Chapter 2: RMS Data Management
- Chapter 3: Master Indices

Core Business Functions

- Chapter 4: Calls for Service
- Chapter 5: Incident Reporting
- Chapter 6: Investigative Case Mgmt
- Chapter 7: Property and Evidence
- Chapter 8: Warrant
- Chapter 9: Arrest
- Chapter 10: Juvenile Contact
- Chapter 11: Field Contact
- Chapter 12: Mental Health Interactions

Analysis & Reporting

- Chapter 13: Analytical Support
- Chapter 14: RMS Reports

Administration & Interfaces

- Chapter 15: RMS System Admin
- Chapter 16: RMS Interfaces

Optional Business Functions

- Chapter 17: Booking
- Chapter 18: Collision Reporting
- Chapter 19: Citation
- Chapter 20: Pawn
- Chapter 21: Civil Process
- Chapter 22: Protection Orders & Restraints
- Chapter 23: Permits and Licenses
- Chapter 24: Equipment and Asset Mgmt
- Chapter 25: Fleet Management
- Chapter 26: Personnel
- Chapter 27: Internal Affairs
- Chapter 28: Registrations

Conclusion

- Chapter 29: Conclusion

TABLE OF CONTENTS

ACKNOWLEDGEMENTS **2**

SPECIAL RECOGNITION **3**

EXECUTIVE SUMMARY **4**

INTRODUCTION **5**

CHAPTER 1 | GENERAL RECOMMENDATIONS **11**

1.1 CHANGE MANAGEMENT 11
1.2 ACCREDITATION 11
1.3 IMPLEMENTATION MODELS 12
1.4 OPEN ARCHITECTURES 14
1.5 SYSTEM ENVIRONMENTS 14
1.6 INTERNAL AND EXTERNAL DATABASES 15
1.7 DATA SHARING 15
1.8 IDENTITY MANAGEMENT 16
1.9 Cross-Module Functionality 16
1.10 Configurability 17
1.11 Attachments 17
1.12 Automated Notifications 17
1.13 SEARCHABILITY 18
1.14 PRINTING 18
1.15 MOBILE TECHNOLOGY 18

CHAPTER 2 | RMS DATA MANAGEMENT **19**

2.1 RMS DATA MANAGEMENT DIAGRAM 19
2.2 DATA ARCHITECTURE 20
2.3 DATA INTEGRATION 20
2.4 DATA STORAGE 20
2.5 MASTER DATA MANAGEMENT 20
2.6 DATA LIFECYCLE MANAGEMENT 20
2.7 DATA OWNERSHIP AND RETENTION 20
2.8 PRIVACY 20
2.9 OTHER CONTROLLED INFORMATION 21
2.10 DATA QUALITY 22
2.11 SECURITY AND COMPLIANCE 22
2.12 AUDITING AND MONITORING 22
2.13 RECORD EXPUNGEMENT, SEALING, AND PURGING 23
2.14 DATA REDACTION 23
2.15 DATA DICTIONARY 23
2.16 DATA MIGRATION 23

CHAPTER 3 | MASTER INDICES 24
3.1 MASTER INDICES DIAGRAM 24
3.2 MASTER NAME INDEX 25
3.3 MASTER VEHICLE INDEX 26
3.4 MASTER PROPERTY INDEX 26
3.5 MASTER LOCATION INDEX 27
3.6 MASTER ORGANIZATION INDEX 27
CHAPTER 4 | CALLS FOR SERVICE 28
4.1 CALLS FOR SERVICE DIAGRAM 28
4.2 NG911 29
4.3 TRANSFER CFS DATA TO THE RMS 29
4.4 TRANSFER RMS DATA TO CAD 29
CHAPTER 5 | INCIDENT REPORTING 30
5.1 INCIDENT REPORTING DIAGRAM 30
5.2 PREPARE INITIAL INCIDENT REPORT 32
5.3 CREATE SUPPLEMENTAL REPORT 32
5.4 REPORT REVIEW 32
5.5 NATIONAL INCIDENT-BASED REPORTING SYSTEM (NIBRS) 33
5.6 USE OF FORCE REPORTING 34
5.7 STOP/PEDESTRIAN REPORTING 34
5.8 CONSENT DECREE REPORTING 34
CHAPTER 6 | INVESTIGATIVE CASE MANAGEMENT 35
6.1 INVESTIGATIVE CASE MANAGEMENT DIAGRAM 35
6.2 ASSIGN INVESTIGATOR 36
6.3 CASE MONITORING 37
6.4 CONDUCT INVESTIGATION 37
6.5 CHARGING 37
6.6 CASE DISPOSITION 37
6.7 NOTIFICATIONS 38
CHAPTER 7 | PROPERTY AND EVIDENCE MANAGEMENT 39
7.1 PROPERTY AND EVIDENCE MANAGEMENT DIAGRAM 39
7.2 COLLECT PROPERTY AND EVIDENCE 40
7.3 VEHICLE IMPOUND 40
7.4 PROPERTY AND EVIDENCE STORAGE 41
7.5 PROPERTY AUDIT AND INVENTORY 41
7.6 PROPERTY AND EVIDENCE DISPOSITION 41
7.7 DIGITAL EVIDENCE MANAGEMENT 42
CHAPTER 8 | WARRANT 43
8.1 RECEIVE AND PROCESS WARRANT 43
8.2 RECEIVE AND PROCESS WARRANT 44
8.3 VERIFY WARRANT 44

8.4 WARRANT SERVICE 44
8.5 CANCEL WARRANT 44
CHAPTER 9 | ARREST 45
9.1 ARREST DIAGRAM 45
9.2 ARREST SUBJECT 46
9.3 WARRANT ARREST 46
9.4 DUI ARREST 47
CHAPTER 10 | JUVENILE CONTACT 48
10.1 JUVENILE CONTACT DIAGRAM 48
10.2 JUVENILE CONTACT 49
10.3 JUVENILE DETENTION 49
10.4 JUVENILE REFERRAL 49
CHAPTER 11 | FIELD CONTACT 50
11.1 DOCUMENT FIELD CONTACT 50
11.2 DOCUMENT FIELD CONTACT 50
CHAPTER 12 | MENTAL HEALTH INTERVENTIONS 52
12.1 MENTAL HEALTH INTERVENTIONS DIAGRAM 52
CHAPTER 13 | ANALYTICAL SUPPORT 53
13.1 ANALYTICAL SUPPORT DIAGRAM 53
13.2 ADMINISTRATIVE AND OPERATIONAL ANALYSIS 55
13.3 TACTICAL ANALYSIS 55
13.4 STRATEGIC ANALYSIS 55
13.5 INTELLIGENCE/INVESTIGATIVE ANALYSIS 55
13.6 FORECASTING ACROSS CRIME ANALYSIS FUNCTIONS 56
13.7 REPORT OUTPUT 56
13.8 CRIME MAPPING/DASHBOARDS 56
CHAPTER 14 | RMS REPORTS 57
14.1 RMS REPORTS DIAGRAM 57
14.2 AGGREGATE REPORTING 57
14.3 PRINTED REPORTS 58
14.4 STANDARDIZED REPORTING 58
14.5 AD HOC REPORTING 58
14.6 DATA QUERIES 58
14.7 CLERY ACT 58
CHAPTER 15 | RMS SYSTEM ADMINISTRATION 59
15.1 RMS SYSTEM ADMINISTRATION DIAGRAM 59
15.2 USER MANAGEMENT 60
15.3 SINGLE SIGN-ON 60
15.4 SECURITY 60
15.5 RMS TABLE MAINTENANCE 61

15.6 RMS CONFIGURATION 61
15.7 GEOFILE MAINTENANCE 61
CHAPTER 16 | RMS INTERFACES 62
16.1 RMS INTERFACES DIAGRAM 62
16.2 CAD INTERFACES 62
16.3 JAIL MANAGEMENT INTERFACES 63
16.4 LOCAL/REGIONAL INTERFACES 63
16.5 STATE/FEDERAL INTERFACES 63
CHAPTER 17 | BOOKING 65
17.1 BOOKING DIAGRAM 65
17.2 PROCESS SUBJECT 66
17.3 VERIFY SUBJECT 66
17.4 RELEASE 66
CHAPTER 18 | COLLISION INVESTIGATION/REPORTING 67
18.1 COLLISION INVESTIGATION/REPORTING DIAGRAM 67
18.2 COLLISION REPORTING 68
CHAPTER 19 | CITATIONS 69
19.1 CITATIONS DIAGRAM 69
19.2 ISSUE CITATION 70
CHAPTER 20 | PAWN 71
20.1 PAWN DIAGRAM 71
20.2 RECEIVE AND PROCESS PAWN DATA 72
20.3 SEIZE PAWN PROPERTY 72
20.4 ANALYSIS OF PAWN DATA 72
20.5 REGIONAL AND STATE PAWN REPORTING 72
CHAPTER 21 | CIVIL PROCESS 73
21.1 CIVIL PROCESS DIAGRAM 73
21.2 SERVE ORDERS 74
21.3 SEIZED PROPERTY 74
21.4 BILLING 74
CHAPTER 22 | PROTECTION ORDERS AND RESTRAINTS 75
22.1 PROTECTION ORDERS AND RESTRAINTS DIAGRAM 75
22.2 PROTECTION ORDER AND RESTRAINT RECORDING 76
CHAPTER 23 | PERMITS AND LICENSES 77
23.1 PERMITS AND LICENSES DIAGRAM 77
23.2 APPLICATION PROCESSING 78
23.3 COLLECTION 78
23.4 BACKGROUND INVESTIGATION 78
23.5 SUSPENSION-REVOCATION 78

CHAPTER 24 | EQUIPMENT AND ASSET MANAGEMENT....79
24.1 EQUIPMENT AND ASSET MANAGEMENT DIAGRAM.... 79
24.2 EQUIPMENT RECEIPT 80
24.3 EQUIPMENT ISSUANCE 80
24.4 EQUIPMENT CHECKOUT.... 80
24.5 EQUIPMENT CHECK-IN 80
24.6 PHYSICAL INVENTORY/AUDIT 80
24.7 EQUIPMENT MAINTENANCE.... 80
24.8 EQUIPMENT DISPOSAL.... 80
CHAPTER 25 | FLEET MANAGEMENT 81
25.1 FLEET MANAGEMENT DIAGRAM 81
25.2 FLEET RECEIPT 82
25.3 FLEET ISSUANCE 82
25.4 FUEL LOG.... 82
25.5 FLEET MAINTENANCE.... 82
25.6 DAMAGE/COLLISION REPORTING 82
25.7 FLEET DISPOSAL.... 82
CHAPTER 26 | PERSONNEL 83
26.1 PERSONNEL DIAGRAM 83
26.2 PERSONNEL INFORMATION 84
26.3 TRAINING AND CERTIFICATION.... 84
26.4 EMPLOYEE PERFORMANCE, SCHEDULING, EXCEPTIONS, AND ADDITIONAL FUNCTIONS 84
CHAPTER 27 | INTERNAL AFFAIRS....85
27.1 INTERNAL AFFAIRS DIAGRAM 85
27.2 REPORTING.... 86
CHAPTER 28 | REGISTRATIONS....87
28.1 REGISTRATIONS DIAGRAM.... 87
CHAPTER 29 | CONCLUSION 89
APPENDICES
APPENDIX A | LIST OF ACRONYMS ....Appendices - 1
APPENDIX B | GLOSSARY ....Appendices - 3
APPENDIX C | END NOTES ....Appendices - 9
APPENDIX D | HELPFUL RESOURCES....Appendices - 10

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 the size or type of organization.

This document serves to provoke thought and careful consideration of law enforcement needs and requirements for an RMS. When procuring a new RMS solution, agencies should prioritize systems built on modern, scalable technology. This includes cloud-based deployment, mobile access, and seamless integration with other public safety systems. The solution should regularly update with new features, security enhancements, and compliance updates to keep pace with evolving technology and regulatory requirements. Agencies should also ensure that the RMS service provider provides a clear, actionable roadmap for future enhancements, guaranteeing the system's long-term viability and alignment with the future needs of law enforcement operations.

Local, state, tribal, and national standards and policies should be considered when implementing a system. Both law enforcement and RMS service providers must understand the impact these policies may have on the RMS, as they vary from agency to agency. Ultimately, each agency should select a solution that best aligns with its specific needs, taking into consideration factors such as agency size, functional responsibilities, and jurisdictional needs.

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 of data entry (i.e., logical edits, edit checks for all fields)
- Ability to configure multi-tier approval processes based on report type
- Configurable permissions to ensure that report access is granted based on a need-to-know basis
- All exchanges generated by an RMS should conform to NIEMOpen standards.
- High level of configurability to alleviate custom development and reduce support.

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.

1.1 CHANGE MANAGEMENT

While not directly related to the functions of an RMS, change management is a critical aspect of any system implementation, and agencies should plan for it accordingly. Change management ensures the smooth and effective integration of changes to software, hardware, and business processes. It is vital to help minimize risks, improve system performance, and support the agency's broader business goals. A structured change management process enables agencies to remain efficient and compliant while adapting to the constantly evolving technological landscape.

Effective change management also includes keeping agency users informed about any changes to business practices that may arise due to the new RMS. Legacy business practices, often based on personal preferences or long-established methods, may need revisiting. When implementing a new RMS, it's an ideal opportunity to review these practices and identify areas where adopting the best practices and new ideas can improve efficiency. Change is necessary for growth and evolution, and the transition to a new RMS provides the perfect moment to streamline operations and align business processes with the new system's capabilities.

Agencies should consider including change management support in their RMS RFI or RFP, asking the service provider to provide services or guidance on implementing and managing change. A well-managed change process ensures that the agency maximizes the new system's benefits while minimizing disruption and resistance to change.

1.2 ACCREDITATION

An RMS that incorporates agency policies and procedures, including accreditation, ensures a structured and compliant approach to managing critical data. The system provides a framework for storing, retrieving, and maintaining records in accordance with legal requirements and internal protocols. Accreditation plays a vital role in validating the agency's

adherence to national or state standards, which ensures that records are handled securely, accurately, and consistently. The agency may want to embed these policies into the RMS, where they can enhance transparency, improve operational efficiency, and foster accountability while reducing the risk of data breaches or non-compliance with regulations. This integrated approach promotes effective governance and supports the agency's ongoing commitment to best practices in law enforcement.

1.3 IMPLEMENTATION MODELS

Overall, there are two primary implementation models for an RMS. These include on-premises 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 agency owns its data, and that the RMS contract includes a clear definition of ownership, a transition plan, and the return of agency data, including metadata, 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. As an agency considers moving to a new provider, a transition plan for migrating legacy data from the old to the new RMS should be in place to ensure successful migration and implementation.

Law enforcement agencies need to remember that regardless of the chosen implementation model, the agency is ultimately responsible for ensuring that their solution complies with the CJIS Security Policy. The agency is always responsible for compliance and audited for it. When implementing cloud services, the cloud service provider may be the most capable of meeting the requirement, but the agency is responsible for ensuring the cloud service provider configures the service to be compliant.

On-Premises Solutions

The following principles define on-premises solutions:

- 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, monitoring system performance, managing user permissions and access control, ensuring compliance with data protection regulations, and troubleshooting issues that arise.
- The agency maintains control of the solution from both a business and technical perspective, which has various degrees of importance and value based on the size and sophistication of the agency.
- The organization is responsible for the storage of data held within the system, including backups and disaster recovery.
- The organization is responsible for managing user permissions and access control, ensuring the solution is only accessed by devices approved to connect to the organization's network infrastructure.
- The organization has full access to their back-end data and can connect to interfaces, reporting tools, and other local cross-platform applications, and the state switch as required.

While on-premises systems have traditionally been perceived as more secure due to direct control over data, they also offer certain advantages that may be relevant for some organizations. On-premises solutions provide complete autonomy over data storage and security, enabling agencies to implement customized controls and policies tailored to their specific needs. For agencies that require strict data governance or have unique security requirements, the ability to manage the entire infrastructure in-house can be a compelling reason to choose on-premises solutions.

With this control, organizations assume responsibility for staying ahead of emerging cyber threats and security vulnerabilities. This necessitates regular patching and timely security updates, which can be challenging if the organization's IT staff lacks sufficient resources or expertise. The agency should also consider the ongoing costs associated with technology updates and data storage.

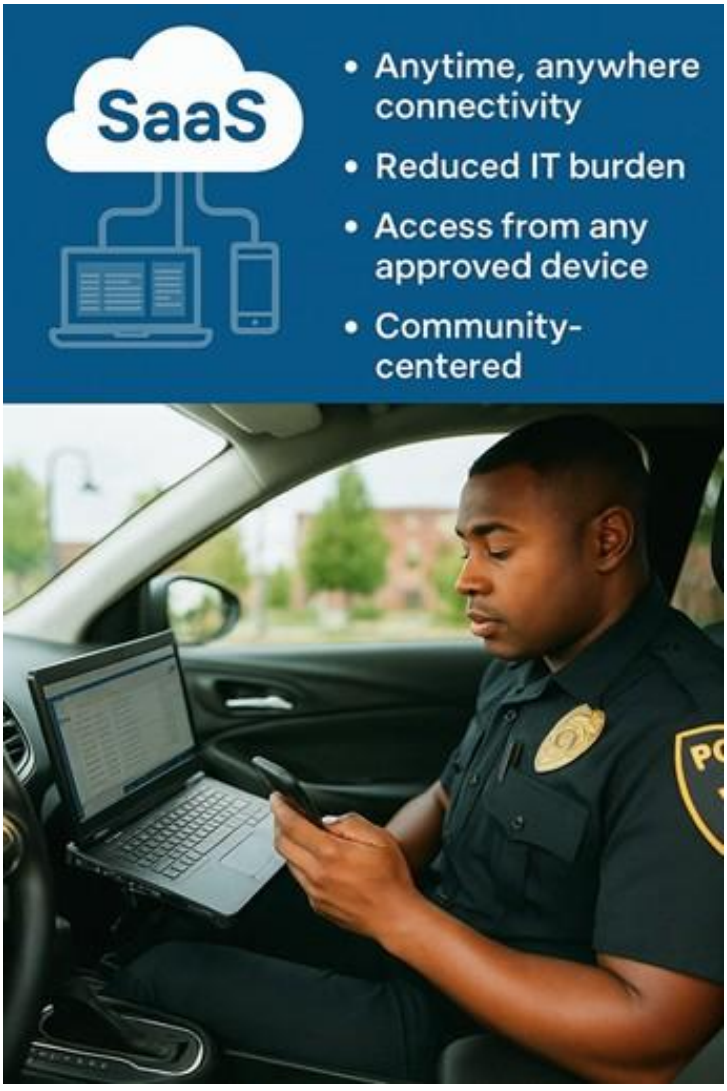
On-premises software solutions can take longer to implement, particularly large-scale systems, and require specialized IT staff for ongoing maintenance and support. Additionally, these systems often demand significant hardware resources, which can add to the overall cost and complexity of the solution. The cost and skillset required to manage and maintain on-premises infrastructure should be carefully considered, especially for organizations with limited resources. Feature and function updates may also take longer to deploy and adopt compared to SaaS models, as on-premises systems tend to be more isolated and require internal testing and integration.

On-premises solutions can offer a strong, reliable option for agencies with specific control, customization, and data sovereignty needs.

Software as a Service (SaaS)

The following principles can define software as a Service:

- The software allows data access from any approved device with an Internet connection and a web browser.
- Service Providers host and maintain the servers, databases, and code that make up the application
- SaaS solutions usually provide just one version of code, but the solution is configurable to accommodate an organization's required branding, etc.
- SaaS products generally operate on a subscription basis, where users pay a recurring fee monthly or annually rather than a one-time purchase, allowing for predictable budgeting and scaling.
- In a SaaS environment, a single instance of the software serves multiple customers to optimize resource utilization and simplify updates and maintenance.



- SaaS providers regularly update their software to introduce new features, improvements, and security patches without requiring users to manage installations or upgrades.
- SaaS solutions can easily scale to accommodate growing operations.
- SaaS providers handle the software's infrastructure, security, and maintenance, allowing organizations to focus on their core activities instead of IT management.

A core principle of SaaS solutions is that they are cloud-hosted, meaning the software and its data are managed and stored on the service provider's servers instead of on local infrastructure. This cloud-based approach offers several benefits, including greater remote accessibility and the ability to share information with other organizations easily. Local agencies access the application via a secure internet connection, enabling them to connect to the system and its data remotely.

Agencies must ensure that the SaaS solution meets security standards, such as the latest version of the FBI's Criminal Justice Information Services (CJIS) Security Policy for U.S.-based organizations or international standards like the UK's National Industrial Security Programme (NISP) for global entities.

SaaS solutions offer significant cost advantages, particularly for agencies looking to minimize upfront and longer-term costs. These solutions typically eliminate the need for substantial capital investment in hardware, as the service provider manages the hosting and infrastructure. Additionally, the need for specialized IT staff to maintain and operate the system is reduced, making SaaS an attractive option for agencies that may not have the resources or personnel to support complex on-premises systems. Deployment is faster and simpler, as agencies do not need to invest in hardware upgrades or worry about ongoing system infrastructure maintenance.

Many agencies also prefer COTS solutions (Commercial Off-The-Shelf) for their SaaS-enabled RMS needs. These solutions are typically preconfigured and ready for quick deployment, reducing both the initial and long-term costs associated with custom development. COTS solutions streamline the implementation process and reduce the complexity of managing software and hardware infrastructure, offering both scalability and flexibility while maintaining predictable maintenance costs.

While SaaS and COTS solutions offer clear cost advantages, such as lower upfront expenses and predictable ongoing subscription and maintenance fees, agencies should carefully

evaluate their specific needs to ensure these benefits outweigh potential challenges. Agencies should verify that cloud-hosted solutions include the appropriate interfaces to connect securely with existing on-premises systems. Additionally, to facilitate seamless and secure data exchange, agencies should thoroughly assess their information-sharing requirements, especially when integration with other internal systems or external partner solutions is necessary.

For agencies that rely heavily on crime analysis, it's important to consider solutions that offer analytical tools, data views, or access to data exports and/or database connections. This is especially important for cloud-hosted solutions, where direct access to the backend database may be restricted.

Overall, SaaS solutions, especially those utilizing COTS software, are highly advantageous for many agencies seeking to reduce capital expenditure and avoid the complexity of managing IT infrastructure. Agencies must carefully evaluate their specific requirements, including security, data sharing, and analytical needs, to determine whether SaaS is the optimal solution for their operations.

1.4 OPEN ARCHITECTURES

When considering an RMS, it is essential 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 architecture is critical to facilitating information sharing across systems. It becomes very important when considering the number of systems an RMS should connect to (i.e., CAD, jail management systems, and other local, regional, state, and national systems). Service-oriented architectures (SOA) and Application Programming Interfaces (APIs) support the need for digital transformation and data sharing. Service-oriented architecture (SOA) is a best practice that supports the decoupling of applications and the 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 are commonly associated with REST/JSON. Regardless of the chosen option, it is essential to remember that resources must 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 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 architecture.

Furthermore, RMS service providers should consider the architecture in their software development efforts to understand where their RMS solutions fit into this bigger picture. They should address how they might expose functionality currently embedded within their RMS to facilitate the implementation of a JRA-based architecture in a jurisdiction. Solutions should be designed with relational data structures to make them easy to understand and maintain. The data structure should be efficient to allow for optimal performance and flexible enough to adapt to changes in requirements, making it easy to modify or extend as new requirements are identified. The data structure should consider a person-centric model that focuses on the individual's involvement across all modules as well as other systems and should be designed to be reusable in different parts of the application. Finally, the structure must be robust, scalable, and maintainable with well-commented code to ensure efficient testing, maintenance, and modification.

1.5 SYSTEM ENVIRONMENTS

Law enforcement agencies must specify whether they require the solution provider to establish multiple environments, such as test, training, disaster recovery, and production. Many agencies prefer to test updates and changes before releasing a new version into production. While this may be time-consuming, it allows the agency to understand the impact of any changes and resolve potential issues before implementation. The agency should also understand the resources required for testing new updates, including the expected frequency of updates.

A quality solution should not require retesting of the entire product with each update. Agencies should work closely with their solution provider to ensure that updates are efficient and do not disrupt normal operations. Additionally, the agency must have a well-defined disaster recovery plan and environment that enables the swift switching of environments in the event of system failure or disaster.

While not as commonly implemented, training environments may be needed temporarily, especially at the beginning of a new implementation. These environments support user familiarization with the system before full deployment and are crucial for smooth adoption.

The type of deployment, on-premises versus SaaS, can significantly impact the complexity and costs associated with system environments. On-premises solutions typically require more agency involvement in managing multiple environments, including testing, training, and disaster

recovery. This may lead to increased costs and the need for dedicated time and resources from the agency to maintain and test these environments. On the other hand, SaaS solutions generally shift the responsibility of managing these environments to the solution provider, potentially reducing the agency's operational burden but requiring alignment on the provider's update and disaster recovery schedules.

Agencies should assess their capacity to dedicate time and resources to managing these environments and collaborate with the solution provider to ensure the environments align with operational needs and security requirements.

1.6 INTERNAL AND EXTERNAL DATABASES

An agency's RMS should support the ability to access and incorporate information from both internal and external data sources where appropriate. Within each module, users should be able to query available agency-approved data systems to retrieve relevant information that supports reporting, investigation, and operational workflows.

The RMS should also allow users to reuse and import data from external sources to reduce duplicate data entry and improve consistency. This includes the ability to compare, validate, and merge data to ensure accuracy and avoid redundancy.

Additionally, the RMS should provide a means to electronically transmit information to authorized external systems in non-proprietary formats. This may occur automatically based on agency-defined rules or manually at the request of the user. Supporting structured data exchange enables better collaboration across systems and helps meet reporting and compliance requirements without requiring manual re-entry of data. The above capabilities should be based on existing resources and criminal justice standards, using NIEMOpen, NIBRS, NCIC, and those developed by the National Institute of Standards and Technology (NIST)[ii].

1.7 DATA SHARING

The RMS should support robust data-sharing capabilities, enabling agencies to exchange information efficiently, both internally and externally. Since the data contained within the RMS is owned by the department, agencies must have the flexibility and control to securely share their data as needed. To achieve this, the RMS should support various integration methods, including Application Programming Interfaces (APIs), standard interfaces, custom-developed interfaces, data exports, and other means of exporting and ingesting data.

APIs and standardized interfaces facilitate secure and streamlined data sharing with other solution providers or partner systems. Agencies may also require custom interfaces tailored specifically to their unique workflows. Data export capabilities ensure agencies can extract information for external analysis, reporting purposes, or mandated data-sharing requirements.

Examples of integration platforms commonly interfaced with include federal and regional data-sharing networks such as the Automated Regional Justice Information System (ARJIS), the FBI's National Data Exchange (N-DEx), NCIS's Law Enforcement Information Exchange (LInX), the Ohio Law Enforcement Gateway (OHLEG). Fusion Centers, and Real-Time Crime Centers. Additionally, critical internal integrations often involve Computer-Aided Dispatch (CAD) systems, Body-Worn Camera (BWC) platforms, Detention or Jail Management systems, Collision/Crash Management systems, E-Ticketing systems, and Court Management Systems. These integrations enhance operational efficiency and support comprehensive data management throughout the agency. See Chapter 16 | RMS Interfaces for additional information.

Agencies may have specific obligations to share data with these systems based on jurisdictional mandates, federal requirements, or interagency agreements. Agencies need to recognize that solution providers or industry partners may impose additional charges for developing, implementing, and maintaining these interfaces. Costs can vary significantly depending on the complexity and type of integration required. For instance, standard APIs or data exports typically incur lower costs. At the same time, custom interfaces, advanced integrations with body-worn camera platforms, detention management solutions, or extensive data transformations may involve more significant investment. Therefore, agencies should carefully evaluate their

integration needs and consider potential costs associated with each type of interface during the RMS selection and procurement process. Ensuring robust interoperability capabilities within the RMS will enhance operational effectiveness, improve intelligence sharing, support advanced analytics, and facilitate compliance with mandatory data-sharing requirements.

1.8 IDENTITY MANAGEMENT

RMS service providers should also consider how to integrate into standards-based ICAM or Identity, Credential, and Access Management frameworks to manage digital identities, their associated credentials, and user access rights. These systems ensure that the right individuals have the appropriate access to the right resources at the right time for the right purposes. Identity management focuses on creating, managing, and deleting user identities to ensure that identity data is up to date and accurate. Credentials such as passwords, biometric data, and smart cards ensure secure access. Access management defines and enforces policies for access to resources based on user identities and their associated credentials. User, resource, environmental, and action attributes are critical in the ICAM process as they are the cornerstone for identification and authorization. These frameworks are, in best practice, part of a security program of the customer, and solution providers should be positioned to integrate into those programs effectively; for example, integrating into an Active Directory store rather than maintaining a separate RMS user store, and ultimately being able to implement SAML or OpenID/OAuth attribute tokens to authorized personnel using Attribute-Based Access Control (ABAC).

RMS solution providers need to consider implementing technology that allows them to receive identity tokens for authorization (and possibly authentication if a separate identity provider does not exist in the customer architecture). OAuth (open authorization), OpenID, and SAML (security assertion markup language) are standard authentication and authorization protocols that enhance security and manage user access to sensitive data. OpenID and OAuth are often used together and are generally well-suited to client-server and mobile application implementations. OpenID is an authentication mechanism utilized to validate a user's identity. At the same time, the OAuth protocol is used to transmit specific attributes about a user and their request for resources or information, on which the application then makes authorization decisions. SAML is well-suited to web-based applications (regardless of platform) and contains both authentication and authorization parts within its standard. These standards allow user authentication across differing organizations and domains. To remain compliant with a changing policy, regulatory, and legal landscape and continue to facilitate effective, secure information sharing, it is important to transition to ABAC, which is an access control paradigm that uses attributes to determine access rather than relying on user roles and permissions. This access control can be facilitated using user and resource attributes tokens. To be a part of this transition, RMS applications should be designed to accept attributes natively in either or both OAuth or SAML formats.

1.9 CROSS-MODULE FUNCTIONALITY

Baseline capabilities should be available across all RMS modules to support consistency, usability, and operational efficiency. These cross-module functionalities ensure that users can perform tasks seamlessly regardless of the type of record or report being worked on. Agencies should expect the following features to be embedded and consistently applied throughout the RMS:

- **Consistent User Interface and Navigation**
  The RMS should offer a familiar, intuitive user experience across all modules to reduce training time and ensure efficient use. Layouts, menus, and data entry fields should follow consistent patterns.
- **Unified Search and Query Tools**
  Users must be able to perform global searches across all modules using names, addresses, vehicles, report numbers, or keywords. The system should also support advanced filtering, saved searches, and layered queries across data types.
- **Role-Based Access Controls**
  Access to records, actions, and administrative tools should be governed by configurable permissions

applied system-wide. These controls must be enforced consistently across modules to protect sensitive data and support compliance with privacy policies.

- **Audit Trail and Logging**
  User actions such as viewing, editing, exporting, and printing should be logged and traceable across modules. This functionality should be standardized to support accountability and investigative review.
- **Attachments and Linked Content**
  The RMS must allow attachments such as documents, images, and multimedia files to be added to any record type. It should also support linking records across modules (e.g., linking a field interview to an incident or a citation to an arrest).
- **Notifications and Workflow Routing**
  The RMS should support automated notifications and task routing for approvals, reviews, or case assignments. These workflows must be configurable and functional across different modules to align with agency processes.
- **Standardized Reporting and Export Capabilities**
  Users must be able to generate reports, summaries, and data extracts from any module using a consistent format. Export functionality should support both human-readable and machine-readable formats (e.g., PDF, CSV, XML, etc.).
- **Spell Check, Formatting, and Narrative Tools**
  Narrative fields, regardless of the module, should include support for spell check, formatting (bold, underline, italics), and standard editing tools. The ability to search narrative fields across reports should also be available.
- **Validation Rules and Error Checking**
  Validation logic, such as mandatory fields, format enforcement, or code table selection, must be applied consistently across modules to improve data quality and prevent incomplete entries.

These functionalities form the foundation of a cohesive RMS platform. Rather than operating as siloed tools, each module should act as a fully integrated component of the broader system, with these shared capabilities enhancing usability, consistency, and operational impact. Several of these topics will be discussed in greater detail in subsequent chapters.

1.10 CONFIGURABILITY

As RMS continues to evolve, there are more opportunities to make features configurable so that agencies can manage the application to meet specific needs. The ability to rename, add, and hide data fields and build agency-specific output forms is highly desirable. Creating required output forms based on data entered in the incident or other reports will streamline agency documentation and reporting. Examples include impound forms, domestic violence reporting forms, summons/complaints, property impound forms, and standard field sobriety test (SFST) forms. Configuring incident and case numbering formats, determining how supplements will be used, setting up property room locations, and adding agency-specific domain values are considered standard RMS requirements over time.

1.11 ATTACHMENTS

Agencies should consider RMS solutions that support multiple types of attachments across all modules. Common attachment types may include victim and witness statements, financial receipts, videos, audio recordings, diagrams, photographs, or other scanned documents. The RMS should allow agencies to define document categories clearly and ensure attachments can be appropriately labeled, categorized, and easily located within the system. At a minimum, attachment titles should be searchable to facilitate quick retrieval and referencing.

When evaluating RMS solutions, particularly cloud-hosted SaaS-based systems, agencies should also consider that storing rich media files, such as audio and video recordings, may incur additional storage-related costs. Understanding and accounting for these potential expenses during the procurement process will help agencies plan effectively and manage long-term costs associated with maintaining comprehensive case records and supporting documentation.

1.12 AUTOMATED NOTIFICATIONS

Given law enforcement personnel's demanding workloads, agencies may benefit from RMS solutions that support multiple notification methods. Agencies should consider systems that allow personnel to subscribe to specific events, enabling notifications related to particular locations,

individuals, or vehicles involved in incidents. Specialized units, such as sexual assault or domestic violence response teams, may benefit from immediate notification when certain types of incidents occur.

Law enforcement administrators should have the flexibility to define notification criteria, recipients, and delivery methods tailored to agency operations. Additionally, the agency may consider automatic notification capabilities for external partners or community stakeholders. Potential notification recipients could include internal personnel, community members, victims, mental health boards, service departments, animal control officers, prosecutors, or other relevant entities. This approach ensures the RMS solution provides adaptable notification options for each agency's unique operational requirements and community partnerships.

1.13 SEARCHABILITY

The RMS should provide robust and flexible searching capabilities, enabling law enforcement personnel to locate and retrieve critical information quickly. Agencies should consider solutions that allow searching on all data fields entered into the system, along with performing cascading or layered searches across multiple criteria. Additionally, the RMS should support keyword and phrase searches within narrative sections, enabling personnel to pinpoint specific details contained in case narratives or reports.

Agencies may also benefit from solutions that allow users to query external systems simultaneously, enabling comprehensive searches across multiple databases with a single action. Enhanced searching allows personnel to rapidly access accurate and timely information, improving operational efficiency, investigative effectiveness, and overall productivity.

1.14 PRINTING

Printable reports should be available for all RMS modules. These reports should be printed with *unapproved*, *draft*, and *official copy* watermarks. The RMS should have the ability for various record release types to omit or include parts of the report, e.g., attachment types or narrative types, to ensure conformance with FBI CJIS and any state/local policies. In addition to the report, the RMS should allow the agency to print all corresponding supplements. The user should be able to choose whether they want to print all or a specific set of supplements. Ideally, these supplements will print automatically in batches 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. The agency should have the ability to save redacted versions of a report. Reports should also be available in a printable document format (PDF).

1.15 MOBILE TECHNOLOGY

Officers should be able to input and retrieve information directly from the field to minimize delays in reporting and improve data accuracy. The RMS should provide this ability while ensuring security requirements related to technology are in place, including Mobile Device Management, device and networking encryption, application and data segregation (such as containerization or application wrapping as appropriate), and private application stores. Agencies should review and understand guidelines for governance and other mobile security requirements based on the data captured and processed by the mobile device. Requirements such as those in the CJIS Security Policy and standards published by NIST for different types of data that may be collected in the RMS are valuable references.

Some service providers have developed smartphone 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 simultaneously. The simultaneous submission of supplements is critical to ensure the rapid completion of reports. Should the device be offline for any reason, the mobile reporting functionality should allow for immediate data upload, including digital files such as pictures and video, when connectivity is available.

CHAPTER 2 | RMS DATA MANAGEMENT

2.1 RMS DATA MANAGEMENT DIAGRAM

A Records Management System (RMS) plays a central role in law enforcement data management. More than just a repository for records, the RMS must support accurate, secure, and compliant data practices that align with agency operations, privacy obligations, and regulatory requirements. Effective data management also requires the system to be configurable, allowing agencies to tailor processes with minimal reliance on the solution provider. This chapter outlines the key components of RMS data management, including foundational practices, lifecycle considerations, and system-level controls. Regardless of the implementation methodology, data management includes the sections that follow.

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 the system, number of concurrent logins, machine used, and duration time-outs
- Report on failed logins, 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

2.2 DATA ARCHITECTURE

RMS data architecture should be designed to support flexibility, scalability, and integration. A well-structured architecture allows for seamless data exchange between modules, clarity in data lineage, and efficient storage and retrieval. Open standards should be used where possible, enabling the RMS to accommodate current and future needs. More information can be found in Chapter 1 Section 1.4 on Open Architectures.

2.3 DATA INTEGRATION

An RMS should support structured data integration with internal and external systems. This includes ingesting data from CAD, Jail, Court, or external partner systems and the ability to export validated data to external repositories. All integrations should use non-proprietary formats and follow industry standards (e.g., NIEMOpen) to ensure compatibility, long-term sustainability, reduce costs, and avoid dependence on a single solution provider.

2.4 DATA STORAGE

The RMS must support secure, scalable data storage that aligns with operational and legal requirements. Whether cloud-based or on-premises, the storage infrastructure should allow for efficient retrieval, tiered access, and compliance with data retention schedules. Consideration must be given to media types, encryption, access logs, and redundancy.

2.5 MASTER DATA MANAGEMENT

Master Data Management (MDM) ensures consistency across core records, such as person, vehicle, property, or location data. MDM helps eliminate duplication and allows related records to be linked correctly across modules. The RMS should support merges, flag, and validation processes that ensure agency-wide consistency in these core entities.

2.6 DATA LIFECYCLE MANAGEMENT

Managing the lifecycle of records is critical for compliance, privacy, and storage efficiency. While archiving may not always be required for SaaS-hosted solutions, the RMS must ensure compliance with state laws and agency-specific policies regarding data retention, archiving, and disposal, including support for expungement, sealing, or redaction based on judicial orders or policy requirements.

2.7 DATA OWNERSHIP AND RETENTION

Data ownership refers to the legal, operational, and ethical rights and responsibilities associated with controlling, managing, and using the data stored and processed within the RMS application. It defines who has the authority to access, manage, and make decisions about the data.

Typically, the agency using the RMS is considered the data owner. Ownership includes the right to control, protect, and decide how data is used, shared, and disposed of. Data applies to all data managed by the RMS. Ownership should be established and documented in the agency's contract with the RMS provider. The contract should explicitly state whether the agency will allow the service provider to share their information, and with whom. The contract should also state that such permission must be renewed on a regular basis as determined by the agency, without relinquishing ownership. The agency should also require that the solution provider share the agency's data and provide a plan for the RMS provider to transfer the data to the agency if the contract is terminated.

The data owner determines who can access and use the data within and outside the agency. Access to the data is typically controlled through role-based permissions and security levels. Regardless of the architecture, the law enforcement agency must remain responsible for data ownership.

Data retention refers to the policies, practices, and legal requirements that dictate how long data within the RMS must be stored, managed, and eventually disposed. It ensures that law enforcement agencies maintain critical records for as long as they are needed for operational, legal, or historical purposes, while also protecting sensitive information from unnecessary exposure or misuse.

A standard police records management data retention policy depends on the type of record, the jurisdiction, and applicable federal, state, or local laws. The system should include a tool to assist the agency with records retention schedule compliance. This would include the ability to predefine retention periods based on the type of case involved and research cases that are eligible for purging. The system should enable the deletion of reports without deleting the corresponding master indices records.

2.8 PRIVACY

Privacy deals with ownership and stewardship of personally identifiable information (PII) within an electronic records system and refers to any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information linked or linkable to a specific individual. This includes both direct identifiers, such as name or Social Security Number (SSN), and indirect identifiers, such as date of birth or biometric data.

Examples of PII:

Direct Identifiers:

- Full name
- Social Security Number (SSN)
- Driver's license or state ID number
- Passport number
- Mobile number

Indirect Identifiers (when combined with other data):

- Date of birth
- Place of birth
- Mother's maiden name
- IP address or device identifiers
- Employment or education details
- Financial account information

Privacy controls must limit access to authorized users and define clear rules for data sharing. The system should capture and enforce these controls across all data stewards. Agencies should also conduct regular privacy impact assessments to remain compliant with evolving laws and regulations.

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

1. The sensitivity of the record is based on the following levels:

   Level 1: All data may be shared
   Level 2: Conditionally shared. System should provide the capability for data contributors to indicate specific elements or record types to be shared.
   Level 3: Not shared. Silent hit sends back notice to the originating agency that a record exists, but the record is not shared.

2. Ability to apply privacy constraints at a data element level using 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 shareable."

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.

PII is protected under various laws, including the Privacy Act of 1974. Several additional references exist, including the Global Privacy and Information Quality Solutions[iv], the Department of Homeland Security, Privacy Office Privacy Impact Assessments Official Guidance, and Chapter 8 of the Fusion Center Guidelines[v]. 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, agency data-sharing agreements will be key to protecting and securing information.

2.9 OTHER CONTROLLED INFORMATION

RMS service providers and law enforcement agencies should be cognizant of rules and regulations governing other types of controlled data such as criminal justice information (CJI) and Criminal History Record Information (CHRI). This data may often be stored within the RMS as supporting documentation for an incident or investigation. The law enforcement agency should be aware of local, state, and national laws and regulations governing the use of this information. Controlled data must be handled securely and responsibly, promoting trust and integrity in the criminal justice system. Agencies should reference guidelines such as the International Organization for Standards ISO/IEC 27001, which provides frameworks for information security management systems that can be applied to protect sensitive criminal justice information. Other standards that govern this information include the FBI's CJIS Security Policy and National Crime Information Center Standards, the Federal Information Processing Standards (FIPS), and the Privacy Act of 1974.

2.10 DATA QUALITY

Ensuring data quality within an RMS becomes increasingly important as jurisdictions utilize it internally for tactical and other analysis and reporting, such as CompStat, and seek to share data between law enforcement and other justice partners electronically. 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. Furthermore, an RMS should implement data quality validations based on context-sensitive business rules. NIBRS validations must be included within the application so that the report can be complete and validated before submission for supervisor review. Other quality checks are necessary. For example, an arrest report must contain an arrest identification number, arrest date, and arrest subject information.

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

2.11 SECURITY AND COMPLIANCE

The RMS should comply with local, state, and federal security and compliance standards. All modules within a single product should be integrated with security rights to define access controls. At a minimum, the RMS must adhere to the most recent version of the FBI CJIS Security Policy, which includes multifactor user authentication, data access and dissemination controls, and data security both in transit and at rest. Each state also has a designated CJIS Security Officer (CSO) who may establish additional policies related to criminal justice data. Law enforcement agencies must understand these policies and ensure their implementation within the RMS.

The CJIS Security Policy is aligned with the National Institute of Standards and Technology (NIST) 800-53 Security Standard, which includes five key elements: identify, protect, detect, respond, and recover. In addition, the solution must comply with other security protocols such as the Driver's Privacy Protection Act (DPPA), 28 CFR Part 20, 28 CFR Part 23, and any state-level laws governing Personally Identifiable Information (PII) and Criminal History Record Information (CHRI), as well as the Health Insurance Portability and Accountability Act (HIPAA). As new laws and regulations emerge, law enforcement agencies and RMS service providers must stay informed of these requirements.

The RMS is also critical for organizing and storing law enforcement data, including case reports, arrest records, and evidence, which enhances data accessibility, improves efficiency in investigations, and ensures compliance with legal requirements. However, as technology evolves, including the integration of AI and other advanced tools, new data security considerations are introduced. Agencies must be mindful of the security risks associated with emerging technologies, such as AI, cloud-hosted solutions, and open-source tools, which may not always meet the high standards required for law enforcement data protection. These technologies, while beneficial, can expose sensitive data to risks like unauthorized access or misuse, necessitating additional security measures, as well as ongoing training and the development of policies for their proper use. Law enforcement agencies must ensure that personnel are well-informed on how to safely interact with these technologies, maintain data security, and follow the organization's guidelines for protecting sensitive information.

International standards such as the UK's MoPI guidance, the Data Protection Act (DPA), and the General Data Protection Regulation (GDPR) may also apply. Depending on the specific agency and jurisdiction, additional security certifications, such as StateRAMP/GovRAMP, FedRAMP, or SOC 2, may be required to meet local, state, or federal compliance guidelines. Agencies should refer to their internal policies to satisfy all security requirements.

To ensure the security of RMS data, agencies should adopt a comprehensive governance framework that includes clear policies for data access, encryption, and secure storage. They must also implement rigorous protocols for auditing data access and usage. Given the evolving nature of data security threats, law enforcement agencies should proactively collaborate with IT, legal, and security teams to stay ahead of emerging risks.

It is important to note that implementing new security requirements or certifications often requires significant investments by service providers, which could result in additional charges for agencies. Therefore, careful planning and budgeting are essential to ensure compliance with evolving security standards while maintaining the integrity of the RMS.

2.12 AUDITING AND MONITORING

Audit logs should be readily available and track all system access, changes to records, data deletions, and report generation/printing. The system should support administrator review of audit trails and provide the tools for administrators to properly review and investigate potential

misuse or threshold violations. Audit data should be immutable and protected against deletion.

2.13 RECORD EXPUNGEMENT, SEALING, AND PURGING

Each state has its own policies for record erasure and expungement, which may impact data retention and reporting. The RMS must support the expungement, sealing, and purging of both entire records and specific data elements within a record. To facilitate this process, the system should allow records and individual data elements to be flagged for restriction or deletion, with the ability to document the reason for restriction.

While the RMS should support expungement and sealing without interfering with NIBRS reporting, some states have requirements that may prohibit continued reporting of expunged or purged data. The system must accommodate these variations based on state-specific regulations.

2.14 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 information that is edited includes victims' names in certain cases, juvenile information, information that the agency considers 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 has already been redacted.

2.15 DATA DICTIONARY

The RMS must provide a capability to display and/or print the relevant database structures, allowing 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:

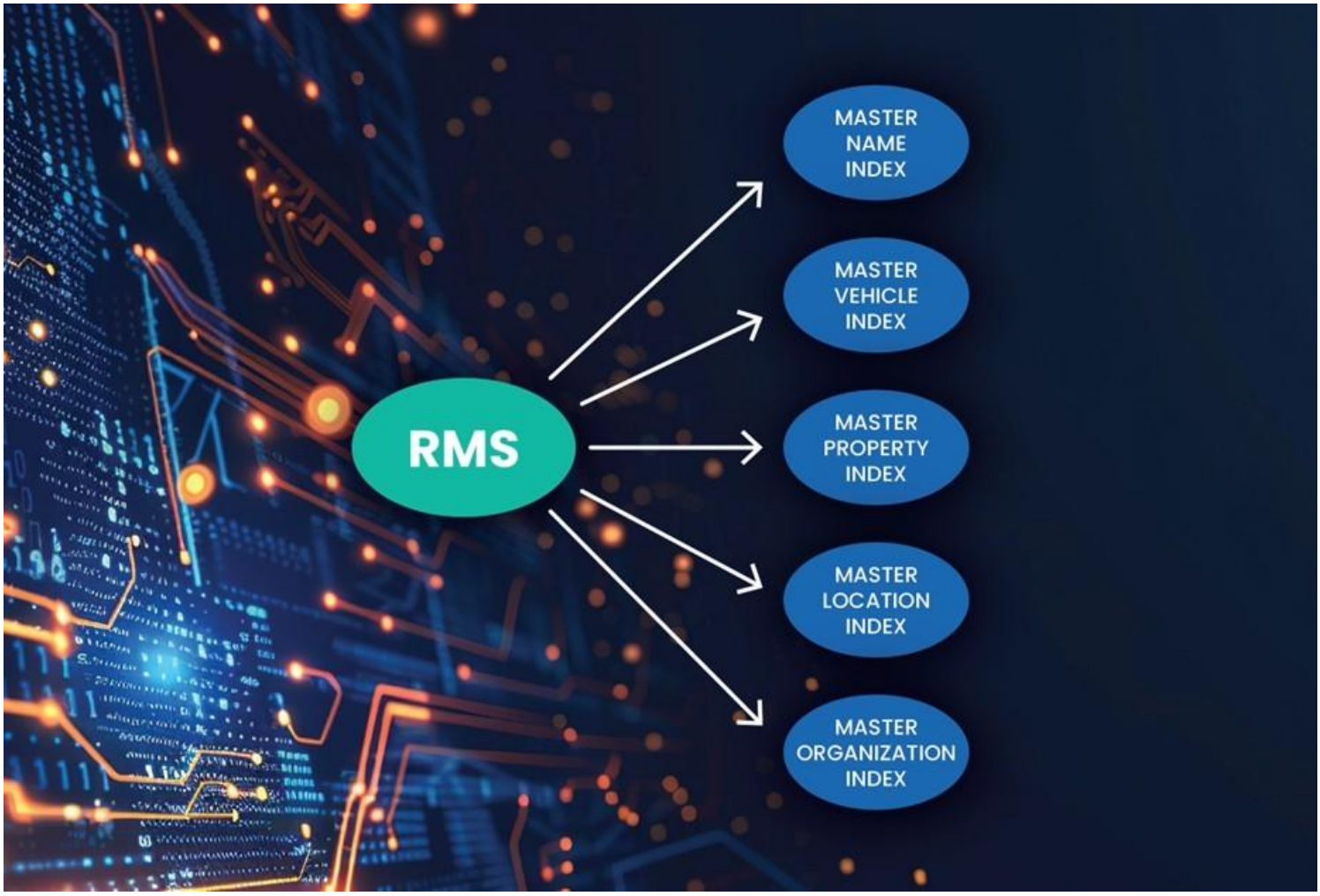
- Field name (e.g., external representation)
- Database column name (e.g., internal representation)
- Data type (e.g., numeric, alpha, or date)
- Field size
- Field format (i.e., output format)
- Edit or validation criteria
- Associated code table
- Default value
- Description

2.16 DATA MIGRATION

The RMS should include the ability to migrate data from the previous RMS, especially if the agency intends to archive the previous data, limiting accessibility. Historical records may no longer be needed for reporting purposes but can be critical to current investigations, such as cold cases. Personnel from multiple law enforcement units, such as Analytical, Investigative, Records, and Accreditation, should be engaged when determining if data will be migrated, data limitations, and impact. The data should be migrated in waves, and continuous testing and validation should be done in the new RMS. Any data gaps, field/structure differences, and impacts on other applications, such as sending data to an information sharing system or utilizing external software for dashboards, should be identified and documented. If data is duplicated in another system for dashboards or analytics, a standard expungement process must be in place to ensure compliance and consistency in the data. The RMS should provide the ability to update or delete previously submitted data to outside systems such as NIBRS, CCH, etc. Agencies and their RMS providers should engage their states to discuss potential impacts when data migration is not included in an implementation. When deciding to migrate data, the agency should also consider the quality of the data contained in its legacy system.

CHAPTER 3 | MASTER INDICES

3.1 MASTER INDICES DIAGRAM



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 that may change over time: an individual's hair color, weight, eye color (contacts), 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 essential characteristics that a master index must have the ability to track.

Master indices' information is captured in various ways, including inputting information into other RMS modules such as incident reporting, collisions, citations, booking, arrests, and juvenile contacts. Additionally, master index data can be imported or shared from external sources such as electronic fingerprinting devices and mug shot systems. Before accepting an entry, the RMS should give the user the option of determining whether there is a match based on existing data. Master indices should not allow automatic updates from external systems without a user review and approval process to ensure data accuracy.

While it is critical to maintain the master index history, law enforcement agencies should be cautious of solutions that automatically combine master index information. Many common names exist, and an RMS may inadvertently

combine unrelated information. Law enforcement agencies must set clear protocols for combining master indices that are true duplicates to ensure accurate master index information. The system should provide a way to undo any erroneous combinations of master indices and have a mechanism to help proactively identify potential duplicates. The system should also allow data removal from an index in the case of expungement or pardon. This should be an automated process driven by an approved user action.

The system should support validating and linking addresses, commonplace names, and street intersections. The RMS must also include linkages among any information contained in the master indices (e.g., people to places or person to person). An RMS should include the ability to create notifications that monitor the master 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. (e.g., trespass warnings, prior domestic violence history, and violent or mental health history).

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, LInX, OHLEG, and N-DEx)
- Prosecution case management system, court case management system, digital evidence management system.
- NCIC
- Nlets
- Computer-aided dispatch (CAD) system

Standard Internal Data Exchanges:

- Existing RMS data
- Digital Evidence/Body Worn Camera Systems
- Property Room Management Systems
- CAD system

3.2 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. By querying that one name, the system can produce a synopsis of all the RMS records associated with that person. It also facilitates linking additional names to an individual master name record (i.e., alias information and relationship data). In querying an individual MNI record, the user would also 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[2], and race. It is vital that RMS adheres to the NCIC/NIBRS standards and any state-specific standards.

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 for the user to assess possible matches, and the user should only match one record to another when confident that they are the same entity.

[2] *This publication fully recognizes the identification of two sexes, male and female, in the Presidential Executive Order "Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government." However, the term "gender" continues to be used throughout this document, as it remains prevalent in the legal language of various state statutes, regulations, and information systems.*

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

Information associated with individuals in the RMS may change, or additional details may become available as new interactions occur. While updates or new information should be captured and linked to existing records, historical data must remain intact, viewable, and searchable. This ensures a complete historical record and facilitates accurate investigative and analytical activities.

Agencies may need to track additional demographic or identifying information, such as whether an individual serves as a primary caregiver or other identifiers such as aliases or alternative identities. The RMS should support flexible methods for capturing these additional identifiers, enabling personnel to document changes or updates accurately as they occur. This helps avoid duplicate records or fragmented data, which could delay investigations or prevent timely access to critical information, such as emergency contacts or reporting requirements to external organizations.

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 by identifying the user of a communication type, those subjects communicating with others through a communication type, where multiple subjects use the communication type, etc.

The RMS MNI should also provide maintenance functions that 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 should also be provided that will allow two or more MNI records to be merged into one record. Unmerge functionality should also allow unlinking two records if it is determined that the records should not have been linked.

3.3 MASTER VEHICLE INDEX

Like individuals, vehicles are often 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 the 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 involving the vehicle. In addition, the RMS MVI may require external interfaces, such as the National Motor Vehicle Title Information System (NMVTIS), state BMV databases, and other data networks.

3.4 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 cataloged 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. If the agency uses a separate solution, property information may need to interface with the agency's property and evidence management system.

3.5 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 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.

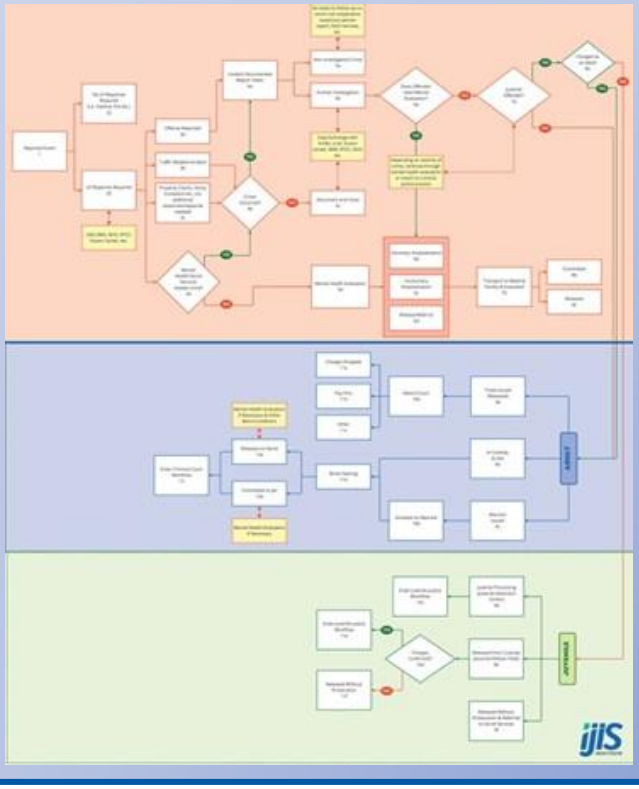
The geo-validation process should allow an address to be accepted, even if it does not appear in the geofile. Unverified addresses should be flagged for possible review. Optionally, either all addresses or only addresses within the jurisdiction are available in the MLI.

3.6 MASTER ORGANIZATION INDEX

Many events 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 various 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 should also 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.

Law Enforcement Workflow

A product produced by the IJIS Institute Law Enforcement Information Sharing Environment (LE-ISE) working group. This group, in collaboration with other national practice associations, focuses on the advancement of information-sharing that is data-driven standards within the LE communities. The current LE information sharing is very valuable to the communities they serve but enhancing data-driven information sharing based on the different types of data can provide the LE agencies with robust capabilities that will help them analyze, disseminate, and act in a timely manner. Through this working group, IJIS Institute members and partners are helping to improve the level of understanding of various types of data that LE has access to, information sharing standards, and create awareness of the need to improve documentation. Check the IJIS website for the latest version of this workflow diagram.



CHAPTER 4 | CALLS FOR SERVICE

4.1 CALLS FOR SERVICE DIAGRAM

All calls for service (CFS) are recorded in a structured records environment in a computer-aided dispatch system (CAD), which allows reports to be run on this data while maintaining a historical record of all calls. A multi-jurisdictional RMS must be able 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. Basic call data (e.g., initial call time, units dispatched, and call disposition) can be used to facilitate the creation of an incident report. Some jurisdictions may allow for mental health tracking; if so, it should be able to start at the call level, allowing users to indicate that the call is or is suspected to be a Mental Health call.

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 when an incident number is assigned or at the initial closing of the call, depending on the specified call types.

If 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 incident number from the CAD system. It is essential to make sure that all responding officers are transferred from CAD to RMS. This helps to ensure a record of all officers at the scene for quality checks related to completing statements and evidence gathering. If the call does not originate from a CAD system, the CFS module should automatically generate or allow manual entry of a sequential event number and an associated incident number to link the CFS and incident records.

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, enroute and on-scene times, 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 Call and Event Data Exchanges to RMS and other external systems

Standard Internal Data Exchanges:

- MNI
- Premise History
- Alerts

4.2 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.

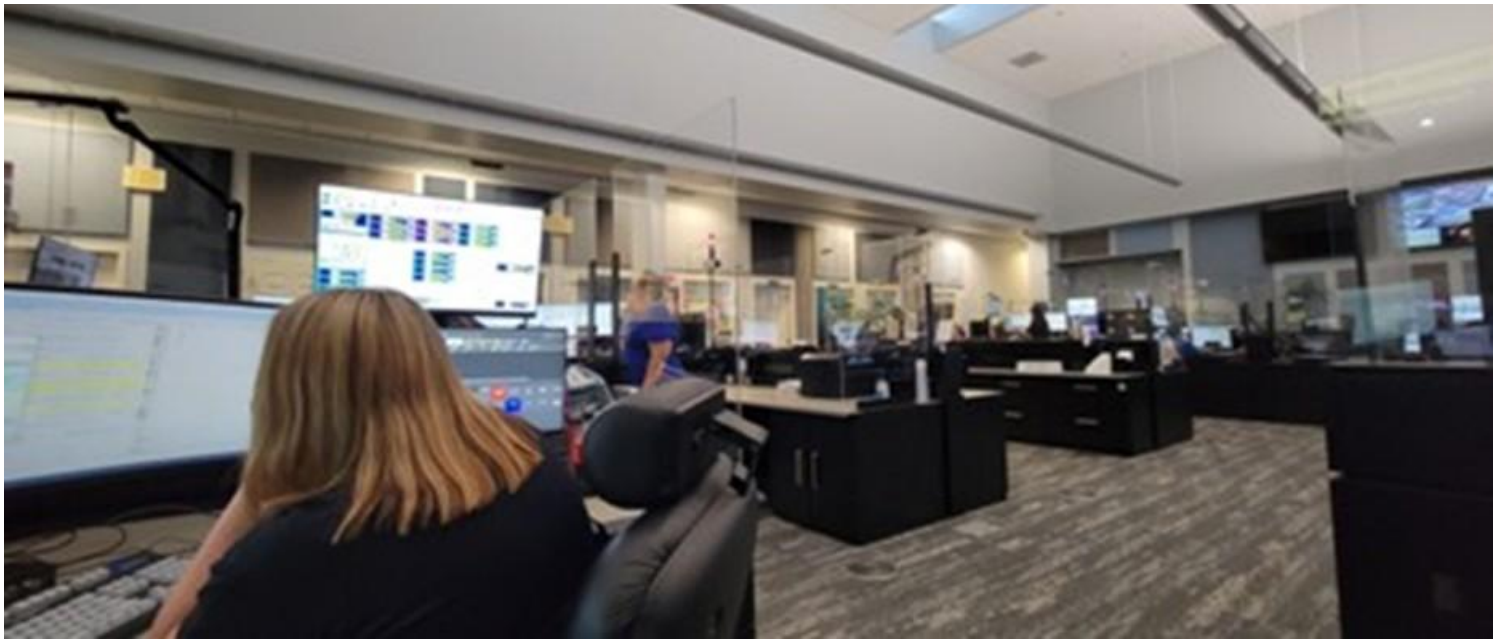
4.3 TRANSFER CFS DATA TO THE RMS

The CAD call data may be transferred to the RMS when units are initially dispatched, after an incident number is assigned, and/or as the call data is updated in CAD.

4.4 TRANSFER RMS DATA TO CAD

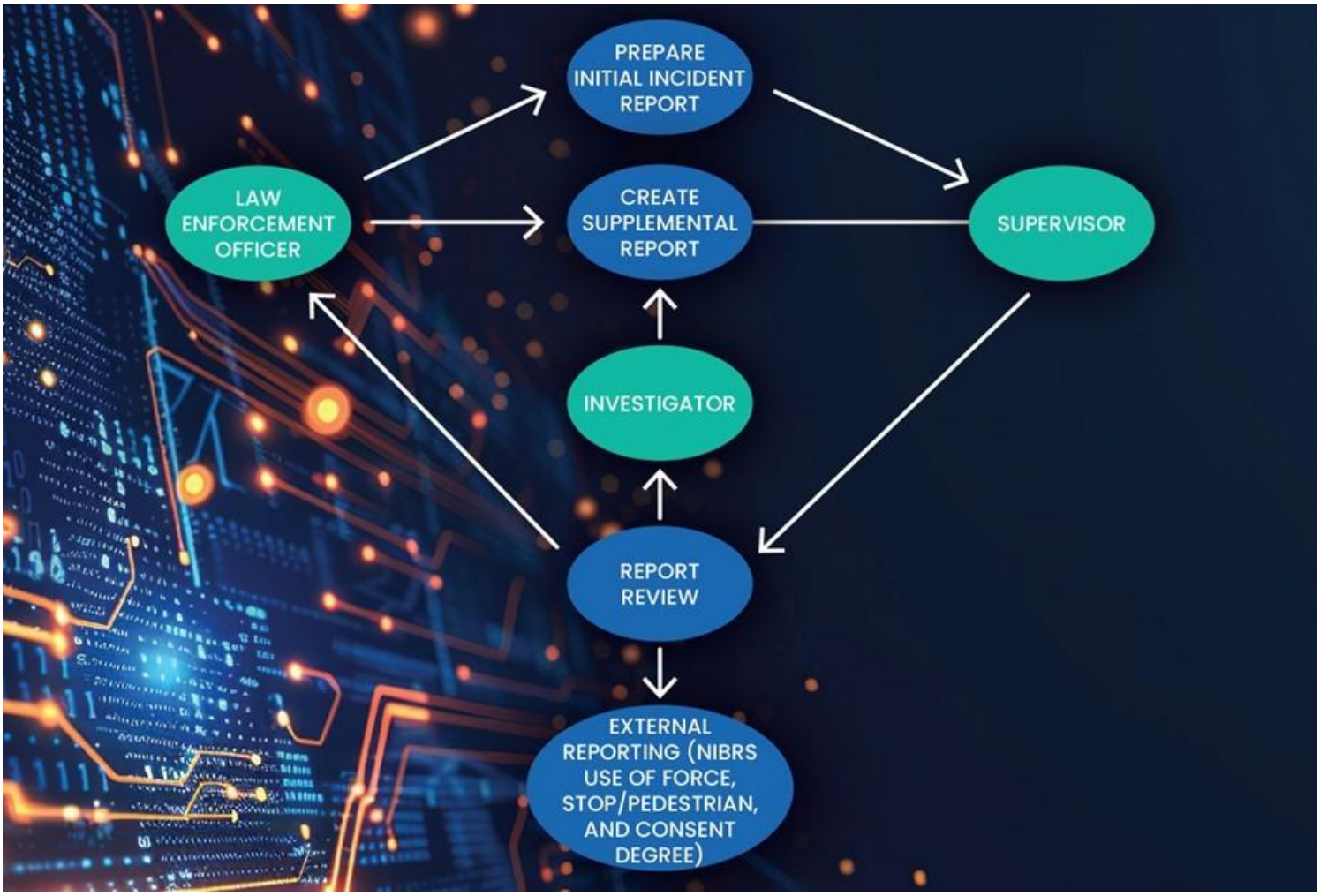
CAD systems should be capable of receiving information from the RMS, such as addresses of known gang members, wanted suspects, and recent violent arrests or domestic incidents, to alert first responders who are dispatched to those addresses.

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 the 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 5 | INCIDENT REPORTING

5.1 INCIDENT REPORTING DIAGRAM



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 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 Program. Every state maintains a state-level incident-based reporting program, which forwards NIBRS data to the FBI. If a state UCR program allows for flat file or XML submission capabilities, the law enforcement agency should require its solution provider to submit data to the state UCR Program in XML format via Web Services. The FBI's N-DEx program is another standard that should be considered within the RMS to allow data sharing across jurisdictions. 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, OHLEG, etc.) 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.

Certain types of incident reports must be available to the public. However, witness information, certain victim information, and the names of juvenile 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 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 on the laws of each state and court orders. In some jurisdictions, there may be a required sealing time period before the records are expunged. It may be helpful if the RMS could include a notification function with the "sealing" function to let administrators know to go back and expunge the data when required.

Generally, sealed records may be accessible to certain people 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 information in the narrative must also be considered. It may be ideal for an RMS to allow for sealing at the field level. For example, a field may be associated with one person that references another person who is sealed. There may be a generic "Notes" field where a user may type something like "parent of John Smith," where John Smith must be sealed.

Certain reports may need to be locked or remain private and accessible only to select individuals in an organization. All copies of the sensitive data must be sealed in the system. This includes Incident data, case data, property/evidence, and even saved PDF copies of reports. These locked reports should not be displayed in search results for people other than those with access to the report. The report must also be removed from and no longer shared with external systems until it is made accessible to the entire law enforcement agency, after supervisor approval.

In addition, the RMS must offer the capability to print a copy of both the full version of the incident report and a redacted version.

Standard Outputs:

- Full and redacted versions of incident reports
- Total incident reports based on period of time, sector, 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 program (NIBRS)
- Prosecutor
- Courts
- Child advocacy centers (Name varies from state to state)
- Jail management system
- State, regional, and federal information-sharing systems and networks [e.g., Nlets, ARJIS, LInX, 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
- CAD
- Online Citizen Reporting Module

5.2 PREPARE INITIAL INCIDENT REPORT

The incident report should be prepared as soon as practical after the incident and may be updated throughout the initial investigation, based on department procedures. Multiple officers may provide input to a single report once it is created and an incident number is assigned. The solution should allow multiple officers to work on a report simultaneously. A primary officer will be assigned with the overall responsibility for completing the report. This primary responsibility may be shifted to other officers during the life of the report. The system should allow a supervisor to easily re-assign a report if issued to the wrong officer in error. Report assignments/reassignment capabilities should be flexible to meet the needs of agencies to manage case assignments beyond the initial report approval process. For example, a report may need to be assigned to a specific division/bureau and then a specific detective or deputy/officer, which isn't always the same as the original reporting officer or known at the time of the initial approval. The incident report must contain sufficient information to comply with state and national reporting standards. The Incident report must be linked to a Call for Service (CFS), Collision Report, Arrest Report, and/or Citation. Ideally, when a Collision Report or Citation results in the creation of an incident report or vice versa, the information taken on the initial report should be transferable to avoid duplicate data entry.

An incident report contains factual information about the incident, including administrative, offense, property, suspect, and case status information, as well as information about witnesses, victims, and complainants. Attachments such as photos, documents, and videos should be supported. These may include financial statements, witness statements, pictures of victims and/or offenders, handwritten notes, etc. The RMS should support linking larger files stored in a digital evidence management system to the incident report.

Reporting requirements typically mandate the collection of certain elements of information. In addition, incident reports have free-text fields, which allow the collection of an unlimited amount of narrative information. The system should provide the capability to search the narratives for a specific word or phrase. Narratives should include spell, and grammar checks and allow for key document formatting capabilities such as bold, underline, italics, etc.

After completing incident reports, officers typically submit them to their supervisors for review. The RMS should automate the review process to route the report automatically through proper supervisor channels. The RMS should allow for re-assignment of report review processes to accommodate when supervisors are out of the office. The RMS must allow the supervisor to reject the report, make changes, or route it back to the reporting officer with notes explaining the reason for rejection. Larger departments may require a multi-stage approval process as dictated by the report type. The report can be directed to the proper supervisors or divisions. In the event the agency maintains a traditional records section that checks reports, 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. It should be noted that some agencies allow for the automatic submission of reports to the state UCR Program once a supervisor approves them and they meet all NIBRS/State-specific data validations.

5.3 CREATE SUPPLEMENTAL REPORT

A supplemental report adds 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, 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, the solution should identify this and automate a process to update the information submitted to the state and FBI. Law enforcement personnel shall electronically submit the supplement report to a supervisor for review and approval.

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

5.4 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 those with access permissions from viewing the document. Locking of the initial incident report typically occurs upon the supervisor's approval. Any information added thereafter is provided as a supplement.

Supervisors are responsible for reviewing incident reports and supplemental reports for accuracy and before their permanent, non-editable storage in the local RMS database. The report may subsequently be distributed to the agency records bureau, other agencies, and local, state, and federal criminal information repositories. The RMS should allow the user and/or supervisor 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 its control. State and local data retention policies should be considered and the RMS should produce reports of potential records that can be purged based on the agency data retention policy.

The RMS should allow supervisors to receive, review, and approve incident reports online and electronically respond to submitting officers and investigators regarding report quality and accuracy issues. The department's standard operating procedures (SOPs) may also require that the records division complete an accuracy review to ensure compliance with reporting requirements before the report is finalized in the system. The RMS should support all required reviews and corrections before 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. When determining the allowable offenses to be reported via the public website, the NIBRS compatibility of the solution used for public submission should be considered. The RMS should allow the submitted information to be automatically created as an incident report for authorized users to review and allocate actions accordingly. Reports submitted via these public citizen-reporting websites must be reviewed by the department before submission to NIBRS and other systems outside of the law enforcement agency for accuracy and compliance. Submission of volume crime reports will enable the public to transact with LEAs without placing additional demand on contact centers.

5.5 NATIONAL INCIDENT-BASED REPORTING SYSTEM (NIBRS)

In January 2021 the Federal Bureau of Investigation's Uniform Crime Reporting Program transitioned from summary-based reporting (SRS) to the National Incident-Based Reporting System, or NIBRS. All law enforcement agencies reporting crime data to the FBI must report under the NIBRS program and format. The traditional SRS program tallied data on crimes in a summary format. NIBRS provides a detailed picture of administrative information, offenses, victims, offenders, property, subjects, and arrestees for each incident reported to law enforcement.

Each state has a state-level repository for the collection of NIBRS data. The state UCR Program is responsible for submitting crime data from all law enforcement agencies within the state to the FBI. Law enforcement agencies and service providers should understand the federal and any state-level requirements involved in NIBRS reporting and ensure the latest version of the FBI/state NIBRS specification is supported. Law enforcement agencies should consider adding language to contracts requiring NIBRS implementation and support and upgrades to the new versions of the State UCR Program requirements at regular specified intervals.

NIBRS provides greater analytical capabilities, including relationships of victims to offenders, location details, and suspected drug and gang activity. The RMS needs to provide NIBRS-defined elements and the values for those elements. It should also include the ability to 'map' state statutes and local ordinances to NIBRS offense codes and update those mappings as defined by the state's UCR program. Offense code tables should support repealed offenses while allowing the offense to be maintained prior to the repeal date. The offense table should also accommodate local ordinances, infractions, and non-criminal report categories.

One key component to successful NIBRS reporting within the RMS is 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 field level via mandatory field validations, pick list confirmations, and conditional mandatory fields, such as requiring entry of property for property-related offenses. There are also specific cross-segment validations that must be included in the validation logic. For example, if an offense is classified as a crime against society, the RMS must ensure that a Victim Type of 'Society' is reported. The RMS should validate incidents in real time and provide clear actions to resolve errors. Ideally, all validations will be included at the officer level to ensure reports are valid prior to supervisor review.

Records staff and administrative personnel should have the ability to review and make data corrections prior to submission of the data to the state program, including the ability to correct NIBRS offense codes within individual reports when necessary. It should be noted that many agencies are moving toward a model wherein the incident report is submitted to NIBRS once the report is approved by the supervisor. If required, the RMS should provide the ability to resubmit corrected data as defined by the state. More detailed information on NIBRS requirements can be found on the FBI NIBRS website. Law enforcement agencies and service providers should contact the State UCR Program for state-specific requirements, as the data is submitted to the FBI through the State UCR Program.

5.6 USE OF FORCE REPORTING

The FBI created the National Use of Force Data collection in 2015 and began collecting data in 2019. The Use of Force specification collects data on the incident, the subject(s), and officer(s) involved. Reporting use of force data to the FBI is open to all law enforcement agencies, and participation is voluntary, not mandated.

The Federal Use of Force program collects data on three types of use of force by law enforcement officers:

- Those that result in the death of the subject
- Those that result in serious bodily harm to the subject
- Those involving discharge of a firearm by LE at or in the direction of a person that did not otherwise result in death or serious bodily harm.

Similar to NIBRS, states may extend the federal Use of Force reporting requirements to collect additional data elements and include validations on those data elements. RMS service providers who intend to support the reporting of Use of Force data to the state and/or the FBI should be familiar with and meet the technical requirements as dictated in the federal or state specification.

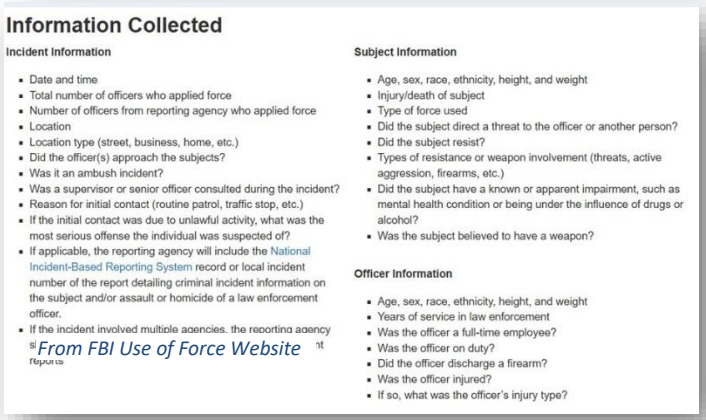
Often, agencies collect data around the use of force that does not meet the requirements mandated in federal or state reporting. This may include uses of force that fall within a defined force continuum, those that result in minor or no injury, uses of mace, deployment of canines, etc. To support that level of use of force reporting, the RMS should provide a Use of Force report that accommodates the ability to define and validate the data collected. The module should include a report submission and approval process, and the ability to include Use of Force reports in internal investigative cases. Use of force data should also be available as a source for internal reporting and analytics to provide agencies with the ability to review what uses of force are being deployed, the success rates of those deployments and what additional training may be needed to either improve use of force deployments or reduce the requirement to use force. More detailed information on Use of Force reporting requirements can be found on the FBI National Use of Force Reporting website.

5.7 STOP/PEDESTRIAN REPORTING

Many states require data collection and reporting for incidents involving traffic or pedestrian stops, as defined by the state. If an agency is mandated to report stop data, the RMS should support the collection, validation, and export of that data according to the requirements of the state program. Stop data should also be available to the agency for internal and/or external reporting.

5.8 CONSENT DECREE REPORTING

A DOJ consent decree is a legally binding agreement between the US Department of Justice and a law enforcement agency. These are usually issued for civil rights violations, misconduct, or other behaviors deemed by the US DOJ as systemic issues within the organization that require change. The consent decree's terms may require the law enforcement agency to produce specific reports to monitor the implementation of the consent decree requirements. If an agency is mandated to provide data about the Department of Justice (DOJ) Consent Decree changes or activity, the RMS should be able to support the collection and reporting of that data as defined by the Consent Decree.


Information Collected

Incident Information

- Date and time
- Total number of officers who applied force
- Number of officers from reporting agency who applied force
- Location
- Location type (street, business, home, etc.)
- Did the officer(s) approach the subjects?
- Was it an ambush incident?
- Was a supervisor or senior officer consulted during the incident?
- Reason for initial contact (routine patrol, traffic stop, etc.)
- If the initial contact was due to unlawful activity, what was the most serious offense the individual was suspected of?
- If applicable, the reporting agency will include the National Incident-Based Reporting System record or local incident number of the report detailing criminal incident information on the subject and/or assault or homicide of a law enforcement officer.
- If the incident involved multiple agencies, the reporting agency si[illegible] nt reports

Subject Information

- Age, sex, race, ethnicity, height, and weight
- Injury/death of subject
- Type of force used
- Did the subject direct a threat to the officer or another person?
- Did the subject resist?
- Types of resistance or weapon involvement (threats, active aggression, firearms, etc.)
- Did the subject have a known or apparent impairment, such as mental health condition or being under the influence of drugs or alcohol?
- Was the subject believed to have a weapon?

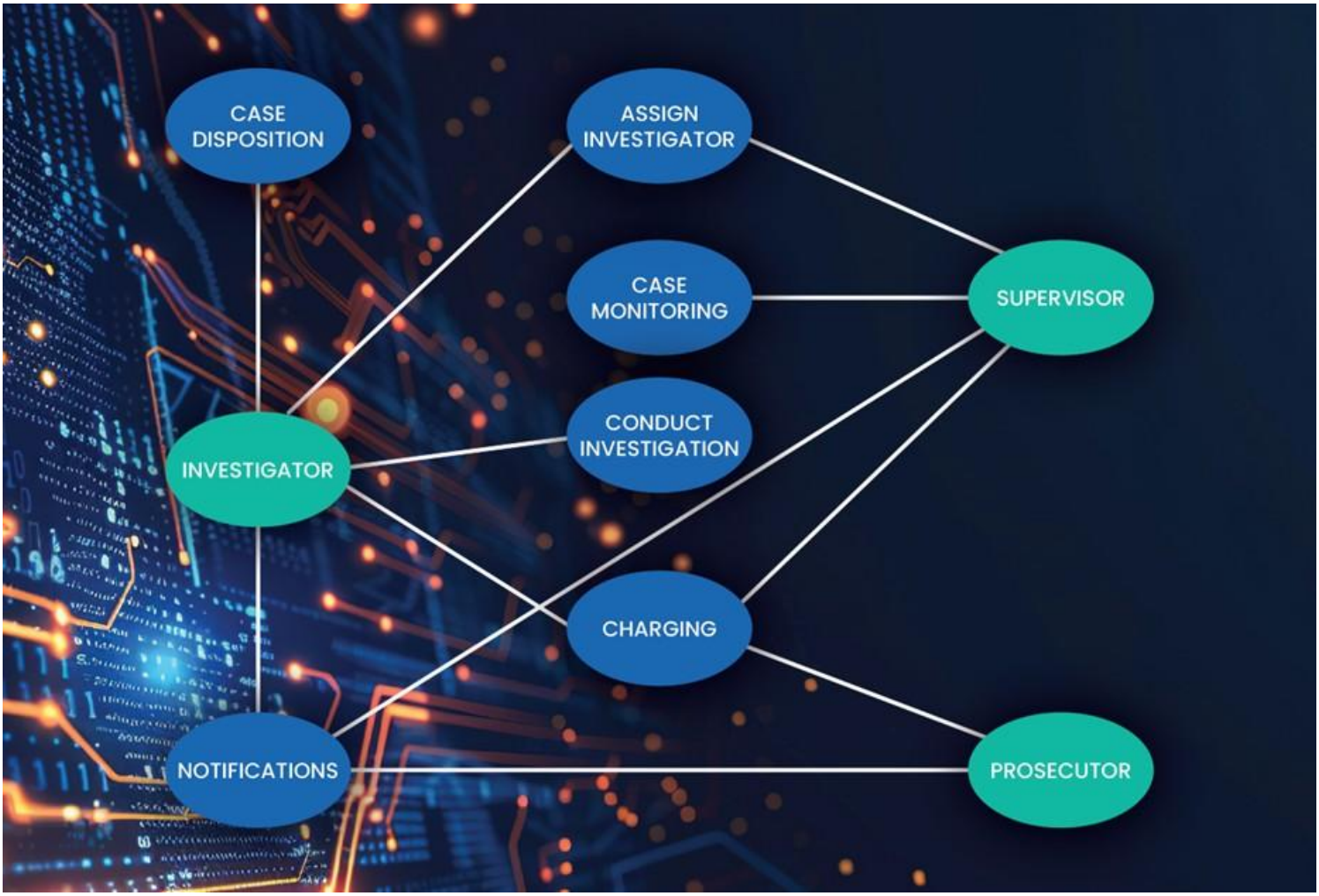
Officer Information

- Age, sex, race, ethnicity, height, and weight
- Years of service in law enforcement
- Was the officer a full-time employee?
- Was the officer on duty?
- Did the officer discharge a firearm?
- Was the officer injured?
- If so, what was the officer's injury type?

From FBI Use of Force Website

CHAPTER 6 | INVESTIGATIVE CASE MANAGEMENT

6.1 INVESTIGATIVE CASE MANAGEMENT DIAGRAM



Incidents requiring further investigation or follow-up may be referred to an investigator before being closed or submitted to the prosecutor for a charging decision. An investigative follow-up case refers to any case that requires additional inquiry or action, such as gathering further evidence, interviewing involved parties, or conducting further investigation or surveillance. Depending on the department's size and policies, the case may be assigned to a patrol officer, typically the one who responded to the original incident, or the department's investigative unit.

The RMS should support the automated assignment of investigative follow-up cases based on configurable business rules such as the type of offense, the status of the incident report, and the agency's investigative units, ensuring that cases are routed to the appropriate personnel efficiently. 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 particular tasks for completion. The Case Management functions should include automated investigative task reminders with due dates and follow-up tasks such as victim interviews, evidence collection, leads collection, expense tracking, preparation of the case for prosecution, and other required tasks. The types of follow-up tasks should be configurable by the agency to meet the specific needs of the investigation. Ideally, the RMS should electronically notify individuals via email or system alerts when tasks are assigned and provide reminders or raise awareness of overdue tasks. In large cases, which may involve hundreds of leads, the investigative module must provide functionality for timely reviews, efficient task assignments, tracking, and prompt dispositions to ensure that all leads are addressed swiftly and effectively.

Case investigations often involve multiple incidents. The Case Management module must allow for tracking multiple

incidents to a single case. Additionally, when an arrest is made, the arrest of one individual should 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 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 may also 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 that 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 completed by all officers, not just detectives. Depending on the size of the agency and policy, minor crimes may be assigned to a patrol officer, typically the one who responded to the original incident, or the department's investigative unit.

Key products of this process include creating arrest reports, clearing multiple incidents from a single case, producing information for prosecutors, managing case materials (including evidence), and preparing cases for prosecution as required.

Agencies should be mindful that these records may be subject to discovery, FOIA, or Public Records Act (PRA) requests and must be managed in accordance with applicable departmental policies.

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, months, 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 (Inactive, Pending, etc.)
- 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, including details regarding potential expungement/pardon business rules)
- State, regional, and federal information-sharing systems and networks [e.g., RISS, Nlets, N-DEx, LInX, 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 - Provide functionalities for managing and documenting the handling of seized assets, including the ability to record transactions, track the status of funds, and generate reports for auditing and compliance purposes.

6.2 ASSIGN INVESTIGATOR

Supervisors must be able to access and review unassigned cases and assign them to a primary investigator. The RMS should allow cases to be assigned to a secondary unit and/or investigator for situations requiring more than one specialized unit. Assignment factors may include the nature of the activity, the type of follow-up required, the workload of available investigators, and cases already assigned. The RMS should allow for the reassignment of cases, especially when the assigned primary investigator is transferred, retires, etc.

6.3 CASE MONITORING

Supervisors monitor cases to ensure that progress is being made. The information used in case monitoring includes case status and activities, 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. If a case involves multiple suspects, the RMS should distinguish the case status related to each suspect.

6.4 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. 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. All case notes and supplemental attachments, such as victim and witness statements, should be printable.

During 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 part of the 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 are described in this report's Property and Evidence Management module section. The arrest process is detailed in the Arrest module.

6.5 CHARGING

When 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 reports, investigator notes, photos, videos, recorded phone calls, victim and witness statements, confessions, and other documents or files pertinent to the case. The system should support the development of charging recommendations and their electronic approval before 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. If mental health information is captured in the RMS, consider how statutes in your jurisdiction may protect that data and the sharing of that data. The detective may file charges or apply for a warrant without making an arrest. Cases may be sent to the prosecutor for a decision before an actual arrest. The system should allow this process to be documented. When a warrant for arrest is issued, the status should be tracked.

Much of the communication between the prosecutor/court and the law enforcement agency in integrated justice systems occurs electronically. The data must be entered manually into the RMS if no interface is available.

6.6 CASE DISPOSITION

In the context of law enforcement follow-up investigations, case dispositions refer to the determination of how a police investigative case is concluded. These dispositions may be based on the outcome of investigative activities, such as arresting a suspect, a decision to suspend the case due to insufficient evidence, or identifying additional leads that justify further investigation. This should not be confused with court or prosecutorial dispositions tied to formal legal proceedings.

When a police investigative case is completed, the law enforcement case disposition should be captured and recorded in the RMS. This may be distinct from and in

addition to the case's activity status (e.g., open, suspended, closed). At this point, any associated property may become eligible for release to the owner, based on an evidence disposition or a destruction order issued by the courts. As defined in the Property and Evidence Management module, preferred workflows should include automatic or manual notifications to evidence custodians to inform them of the investigative case disposition and support the proper handling of evidence.

Separately, court dispositions associated with each individual arrested and per charge may also be captured in the record once the legal process is complete. In an integrated justice environment, these dispositions can be received electronically through interfaces with court or prosecutor case management systems.

The RMS should also support reopening a follow-up case when new evidence emerges and allow for configurable business rules related to the record expungement, ensuring compliance with legal and policy requirements.

6.7 NOTIFICATIONS

Effective communication throughout the investigative process is essential for maintaining case continuity and ensuring timely action. Agencies should consider RMS solutions that support automated notifications to alert personnel of key events or updates related to a follow-up investigation.

When a case is open and new information is added, such as evidence, reports, property, or other case-related materials, a notification should be sent to the assigned investigator. If the case is already closed and an item is added, the system should notify the assigned investigator and the current unit supervisor to ensure proper awareness and follow-up.

Depending on the agency's workflow and technical environment, notifications may be delivered through various channels, including electronic system alerts, email messages, task notifications, or other suitable warnings.

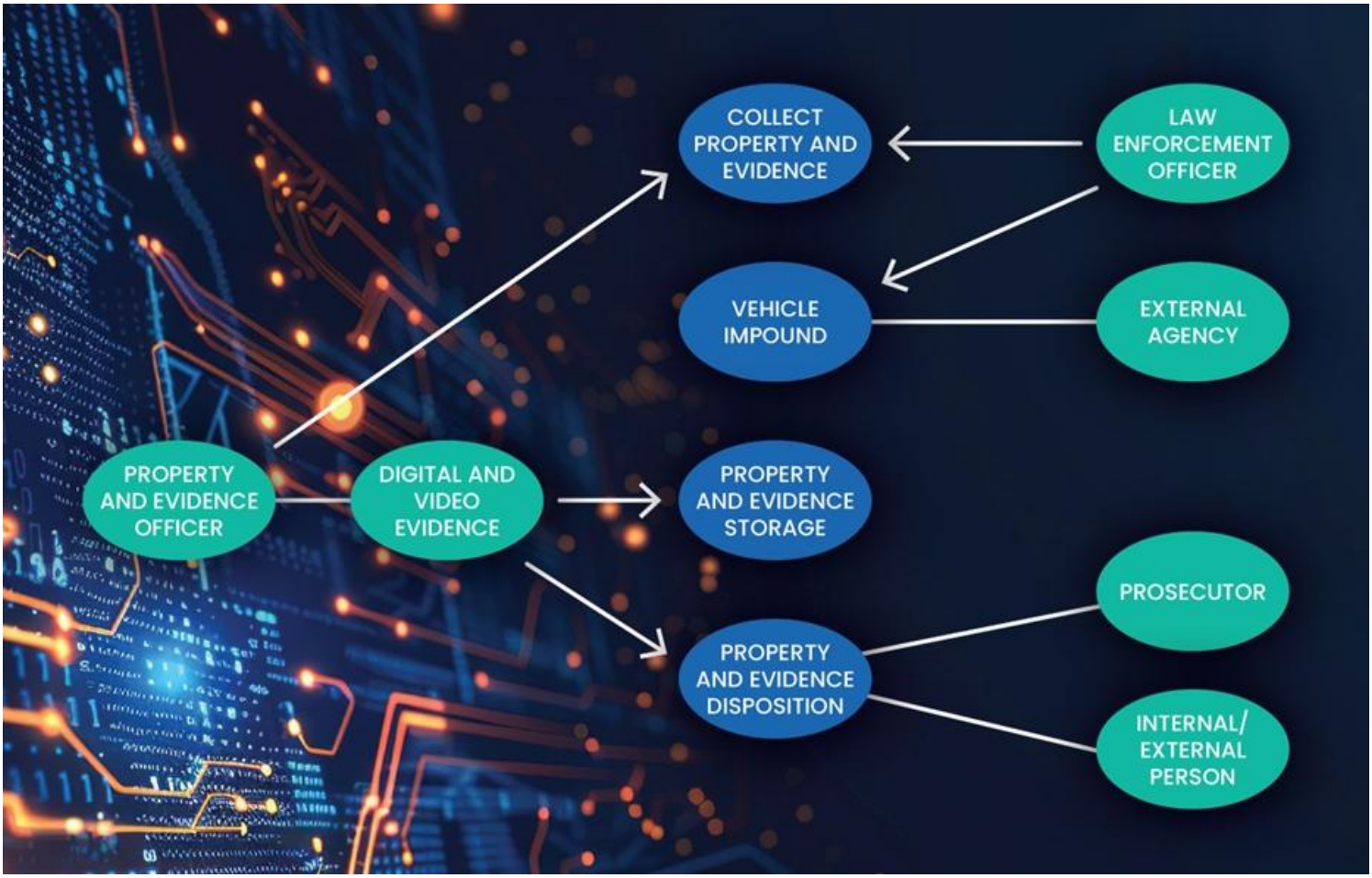
In addition to property and evidence updates, other events that may warrant notifications include:

- Assignment of a new investigative case
- Updates to an existing case or associated reports
- Submission of a new incident report that may require investigative review
- Reassignment of cases between investigators or units
- Assignment of specific follow-up tasks or activities
- Receipt of a prosecutorial or court disposition
- Reopening of a case based on new evidence or developments

Supporting timely and flexible notification workflows improves investigative efficiency, promotes accountability, and ensures critical updates are promptly acted upon.

CHAPTER 7 | PROPERTY AND EVIDENCE MANAGEMENT

7.1 PROPERTY AND EVIDENCE MANAGEMENT DIAGRAM



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 according to agency policy. Field personnel should also be able to enter data into the Property and Evidence Management module remotely, allowing documentation to occur in real time while in the field.

The Property Module should track each property item's complete chain of custody. Property recorded in an incident report should seamlessly transfer to the Property Custody module without requiring duplicate entry. Some law enforcement agencies use temporary lockers for property storage before the final check-in by the property custodian, and this process must be recorded as part of the chain of custody. The location of all seized, impounded, or stored property should always be searchable.

Search results should, at a minimum, display an item's current status or location, description, date received, and reason for receipt. Personnel should also be able to follow links to related property records within the system. Additionally, property and evidence information must be linked to a case file or report detailing the circumstances under which the department received the item.

The system must manage property disposition, including notifications for property custodians, and provide search functions to identify items eligible for release, destruction, or auction. Disposition history may be maintained for a specified period or retained indefinitely for future investigations. The system should also support digital signatures or biometric authentication to document property release or transfer.

Many jurisdictions use stand-alone software programs for property and evidence management. If the agency uses stand-alone property management software, property reported for NIBRS must be included in the RMS or transferred to the RMS via an interface. The RMS must offer standards-based interfaces to integrate with these systems and allow data imports using standard file formats. Additionally, links to appropriate RMS records should be created when property records are uploaded.

Standard Outputs:

- Chain of custody
- 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
- Vehicles impound forfeiture report
- Case closed evidence report
- Evidence location summary report
- Audit reports
- ATF gun trace form
- Other commonly used forms

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, prosecutors, coroner's office, and courts.

Standard External Data Exchanges:

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

Standard Internal Data Exchanges:

- Incident Reporting module
- Fleet Management module

7.2 COLLECT PROPERTY AND EVIDENCE

Property and evidence items are collected and processed in 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. The system should support the use of barcode and/or RFID technology to streamline the check-in and check-out process and ensure accurate tracking of the chain of custody. A single item or multiple items (batch) may be moved in one transaction.

7.3 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 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 vehicle's condition, 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 following NCIC standards.

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

At the impound facility, the owner and driver information, 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.

7.4 PROPERTY AND EVIDENCE STORAGE

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

7.5 PROPERTY AUDIT AND INVENTORY

The property room inventory needs to be audited regularly 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 audit date. 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 a barcode scanner. Law enforcement agencies should ensure that property audits conform to 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.

7.6 PROPERTY AND EVIDENCE DISPOSITION

The final disposition of property is essential to maintaining manageable storage capacities for the agency and allowing certain owners to have their property returned promptly. The disposition process documents the disposition action and includes safeguards to ensure that procedures and laws governing the item's release, sale, or destruction are followed. The system will use timed events, such as system messages or providing access to lists of eligible property items, to notify the property custodian when the 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 before the disposition. It may also 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 individual's identity 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 before the release of the property. The property is eligible for sale or destruction after a prescribed

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

7.7 DIGITAL EVIDENCE MANAGEMENT

Digital evidence refers to information that is stored, received, or transmitted by electronic devices. It plays a critical role in modern investigations and can include digital images, audio and video recordings, forensic copies of computer drives, and data from surveillance systems or body-worn cameras. This type of evidence may come from a wide variety of sources, such as hard drives, cell phones, USB drives, flash memory cards, or cloud-based storage. For digital evidence to be admissible in court, it must be carefully collected, preserved, and secured throughout the investigation process.

Because of the sensitivity and data storage requirements of digital evidence, along with the wide variety of sources it comes from, many agencies use dedicated digital evidence management systems. These systems are designed to store large amounts of digital content, maintain a secure chain of custody, and ensure the original files remain unchanged. They also track who accesses the files, capture metadata, and control user permissions to ensure that only authorized personnel can view or manage the evidence. These systems help ensure that only authorized personnel can view or manage the files and that everything is documented for legal proceedings.

It is important to understand that most records management systems (RMS) are not designed to function as digital evidence systems. While an RMS may support attaching items like photos, scanned reports, or videos to help tell the story of an incident or case, this content is generally not intended for evidentiary use. The purpose of including these files in the RMS is to enhance decision-making and provide better visibility of what happened. Digital evidence that must be preserved for trial or investigation should be stored on approved digital media or within a dedicated evidence management system, in accordance with your department's policies and procedures.

It is important that an RMS supports connections to digital evidence management systems. This allows agencies to link records, cases, or incidents in the RMS to the corresponding digital evidence, without storing the actual files within the RMS itself. In some situations, this may involve tagging records to reference related digital evidence or importing key metadata from the external system. The goal is to maintain a clear distinction between operational records and evidence that must be preserved for legal or investigative purposes.

Just like any other form of evidence, digital content must be handled with proper access controls, retention policies, and audit trails. Storage systems for digital evidence should be treated with the same level of care as physical property rooms, with all actions tracked and secured. Agencies should also be able to share digital evidence with prosecutors and defense attorneys through controlled, read-only access when appropriate.

The RMS plays an essential role in supporting law enforcement operations, but it is not a substitute for a purpose-built digital evidence management system. When used together, each system can perform its intended function, one for organizing and understanding information, the other for protecting and preserving evidence throughout the justice process.

7.8 DASHCAMS AND BODY-WORN CAMERAS (BWC) USAGE

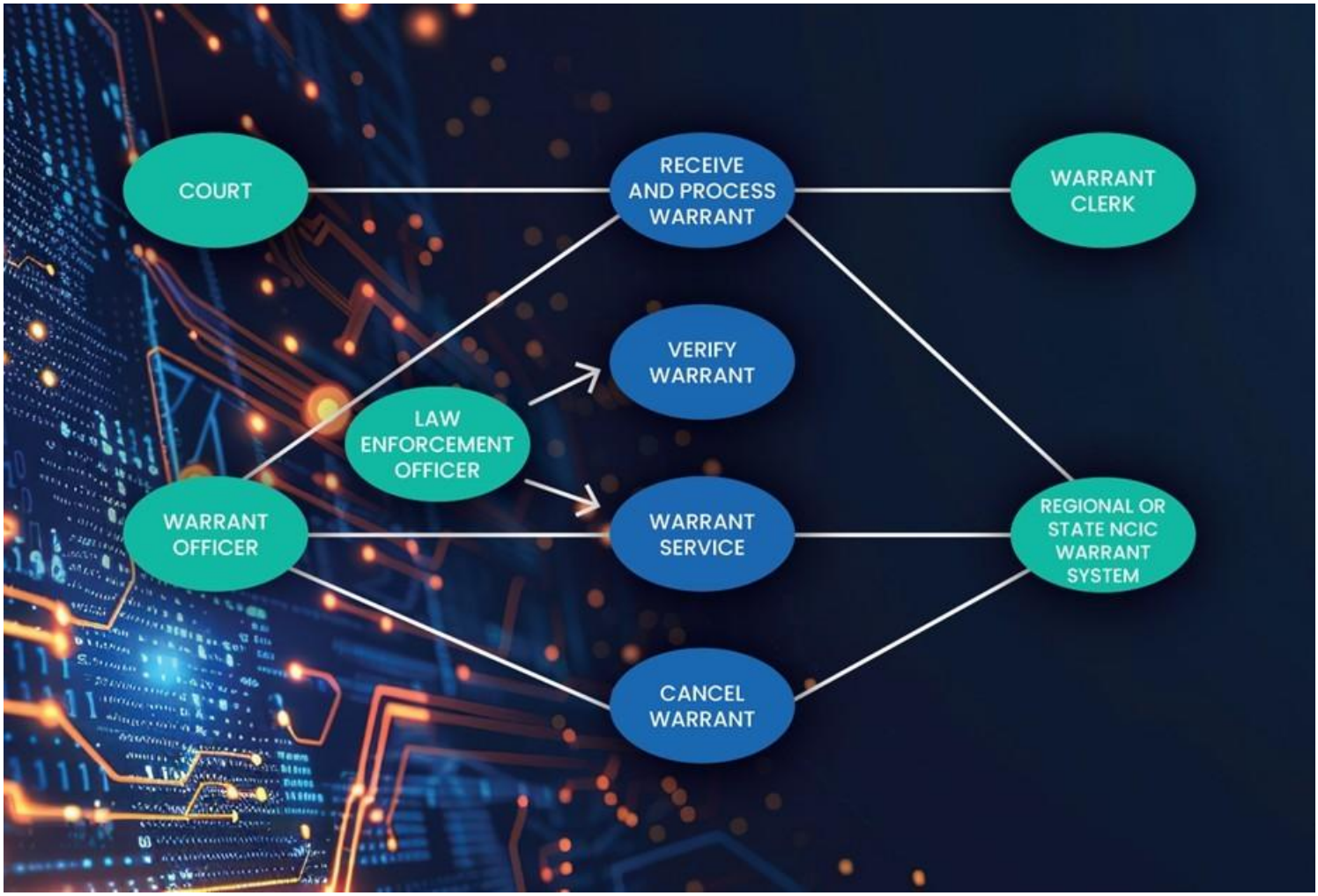
Dashcams and body-worn cameras (BWC) play a critical role in law enforcement by providing objective video evidence that supports transparency, accountability, and the accurate documentation of incidents. The footage captured can be instrumental in investigations, legal proceedings, and internal reviews and is considered a form of digital evidence. If agencies consider adopting AI tools to interpret body-worn camera footage, it is critical to ensure proper policies are in place to govern the use of these tools. When adopting AI tools to generate report narratives, the policy must dictate that the officer review and sign off on the report narrative.

When filing reports in the Records Management System (RMS), it is essential to note the existence of any related dashcam or BWC footage. This ensures that all evidence is accounted for and easily retrievable when needed. Proper documentation should include details such as the date, time, and nature of the recorded event, along with any relevant identifiers.

To enhance efficiency and accuracy, the RMS and, where applicable, the Computer Aided Dispatch (CAD) system should support interfaces that enable seamless integration with video management systems. This functionality allows for the automatic tagging of video files to the corresponding call for service and police incident report. Such integration reduces the risk of misfiled evidence, improves data integrity, and streamlines the process of retrieving video during investigations.

CHAPTER 8 | WARRANT

8.1 RECEIVE AND PROCESS 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 who 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 a warrant is not an arrest until a physical arrest is made. The court must approve the warrant request, and then the individual must be served and arrested before the arrest is recorded in the RMS. When applicable, the RMS should generate a warrant request based on data available in the incident and an arrest report.

Standard Outputs:

- Warrants issued
- Warrants served or cancelled
- Warrant summary based on varying search criteria
- Attempts to serve by date or date range
- Warrant aging report
- Warrant affidavit complaint

Standard External Data Exchanges:

- Courts
- Prosecutor (for extradition determination)
- Regional, state, and federal warrant repositories following NCIC standards
- State, regional, and federal information-sharing systems and networks (e.g., RISS, Nlets, ARJIS, LInX, OHLEG, N-DEx, ISE)
- Jail management system
- Corrections
- Mobile computing systems

Standard Internal Data Exchanges:

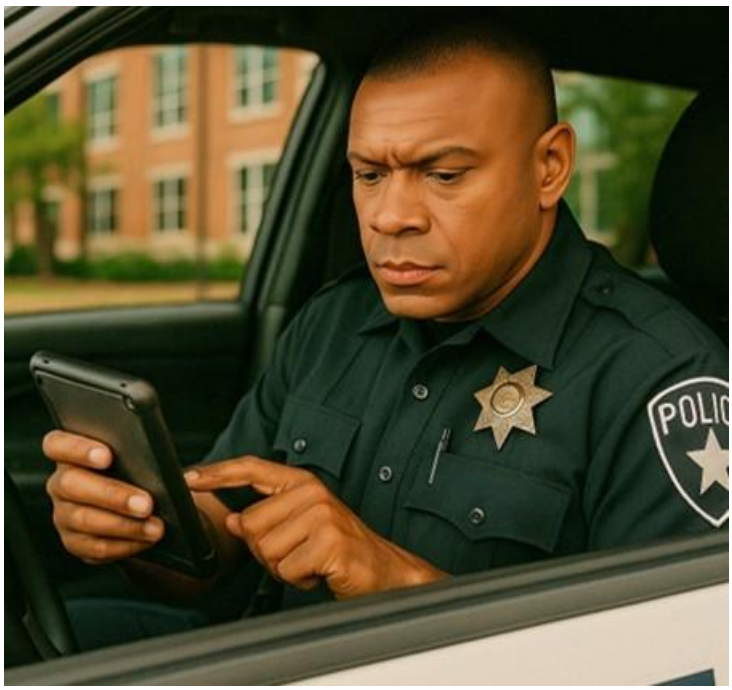
- Booking
- Master Name Index
- Master Vehicle Index
- Master Property Index

8.2 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 should update the appropriate regional and/or state warrant systems. The warrant clerk reviews the warrant for completeness and ensures the subject information is current.

8.3 VERIFY WARRANT

Immediately before 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. Verifying whether the warrant has been canceled (dismissed or recalled by the court) or served by another external agency is critical. This warrant verification process is also important in determining whether the wanting agency will extradite the subject if the warrant is served.

If available, the verification can be done using a mobile data computer with the appropriate interface. Alternatively, the officer can contact dispatch or another department facility to have the warrant verified.

8.4 WARRANT SERVICE

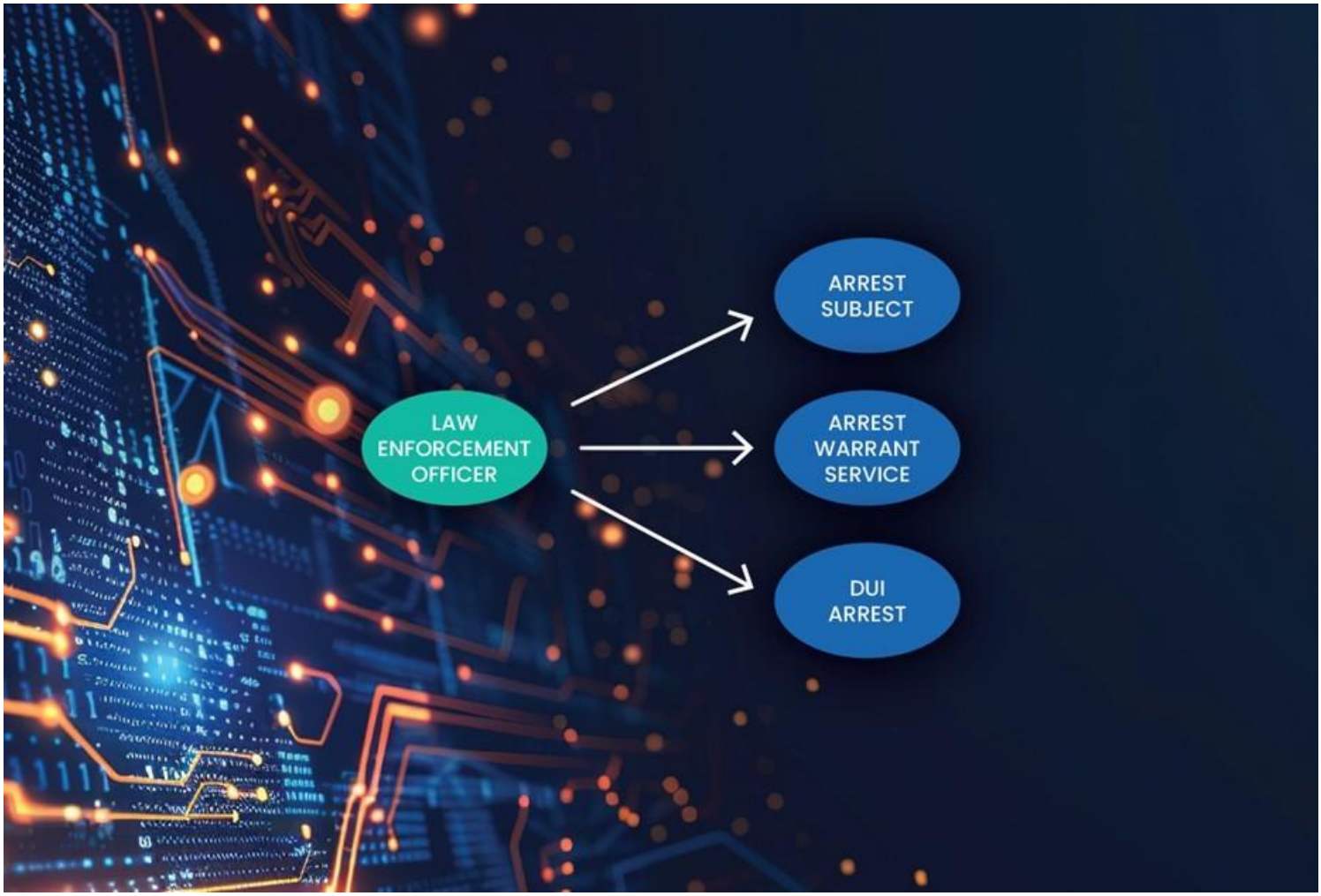
The process of serving a warrant varies based on the type of warrant. The Warrant Module tracks and records all warrant-related activities and status changes. Each activity is documented with details such as the type of activity, any contact with the subject, service of the warrant by an external agency, the date of the activity, and the outcome. Once the warrant is served, the module is updated, and the warrant is cleared in the appropriate warrant systems. A warrant is considered cleared when the person wanted is apprehended. A warrant is considered cleared when the individual named in the warrant has been located and taken into custody.

8.5 CANCEL WARRANT

The court has the authority to cancel a warrant, and the reason for cancellation must be documented in the Warrant Module. Other relevant warrant systems must be updated, either manually or through an interface, to reflect the cancellation. Proper documentation ensures accurate records, prevents unnecessary enforcement actions, and maintains compliance with legal and procedural requirements.

CHAPTER 9 | ARREST

9.1 ARREST DIAGRAM



Law enforcement agencies arrest subjects suspected or charged with committing a crime. Arrest actions must be supported by either probable cause existing at the time of arrest or a court warrant signed by a judge commanding the subject's arrest. The arresting officer must follow well-defined procedures, which include accurately documenting and recording every step in the arrest process. Once the person is arrested, both scenarios follow the same procedure.

The Arrest module provides a place to document all steps taken during an arrest, with this complete documentation serving as a critical component in defending the legality of the arrest.

In many systems, the Arrest module initiates or feeds data into a Jail/Detention Management system for an arrested individual's incarceration, booking, or short-term holding. This module is typically separate from the incident reporting module, ensuring that arrest-related data is properly tracked and handled independently. The data entered in the Arrest module should be easily linked to the original incident or case, allowing the data to seamlessly flow to other modules such as the Booking module, the jail management system, the prosecutor, and the courts. To avoid duplicate entry and ensure proper tracking, the incident and arrest modules should be tightly coupled so that both the arrest and corresponding incident are clearly identified, linked, and common data shared. Furthermore, any data entered in the Arrest module should be reusable across other modules, enhancing efficiency and ensuring data consistency throughout the system.

Integrating the Arrest module with other systems ensures that all relevant information is accessible and up-to-date, reducing errors, eliminating redundancy, and improving overall case management. This seamless flow of information

supports the effective management of arrests, bookings, and ongoing case investigations, ensuring that all parties involved have the necessary data to make informed decisions.

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
- 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
- Ability to populate required forms (Miranda, OUI rights, property, etc.) using system data

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

9.2 ARREST SUBJECT

When a law enforcement officer secures a subject, they may take the individual into custody if circumstances justify continued detainment to ensure public safety and maintain order. A probable cause or on-view arrest occurs when sufficient evidence supports the officer's actions based on the immediate circumstances of an incident. This includes cases where the officer directly witnesses a misdemeanor crime (on-view arrest) or has enough evidence to determine that a crime has been committed. In some instances, the arrest may initiate the detention and booking process.

Law enforcement officers should make every reasonable effort to confirm a subject's identity before taking them into custody. The system should provide automated alerts for any outstanding warrants and/or alerts associated with the subject. The Arrest module should allow officers to document the method of identification used and record the completion of key steps, such as issuing the Miranda warning. This information will be included in the officer's incident report, with additional details captured as needed for NIBRS reporting.

The RMS must provide the capability to generate an arrest report once all required data has been entered. An arrest report is necessary when an officer completes the arrest process by transporting a subject to jail. Additionally, the RMS should support and document the agency's arrest report review process.

The system should also accommodate cite and release arrests, where a person is taken into custody for a misdemeanor offense but is not booked into jail. Instead, they are issued a citation with a notice to appear in court. In some circumstances, these citations may be NIBRS reportable offenses. Integration with a booking and/or jail management system may also need to be considered.

9.3 WARRANT ARREST

An arrest based on a warrant can occur in two situations. First, a law enforcement officer may execute an arrest warrant issued as a result of an ongoing investigation. These warrants are based on charges approved by a prosecutor or court, signed by a judge, and specify whether the subject is to be held with or without bond. The warrant should also indicate whether it can be served during the day, at night, or at any time. Charges listed in the warrant may or may not be updated before its execution. Once served, the arrest follows the same process as a probable cause arrest.

The second situation occurs when a law enforcement officer conducts a warrant check during a traffic stop or other routine activity and discovers an active warrant for the individual. Before serving the warrant, the officer must verify its validity. If another jurisdiction issues the warrant, the officer must confirm whether the issuing agency is willing to

extradite. This verification process can often be completed using a mobile data computer with the appropriate system interface.

Many agencies require an incident report to document the circumstances of an arrest, including taking the subject into custody, transporting them to the detention center, and releasing them to staff without incident. However, some agencies do not require a formal arrest report for warrant-based arrests, particularly when the subject does not resist. Officers should refer to their department's Standard Operating Procedures (SOP) for specific reporting requirements.

Once the warrant has been executed, the RMS should support or integrate with the Case Management System (CMS) to ensure the warrant is marked as served and removed from all relevant warrant databases.

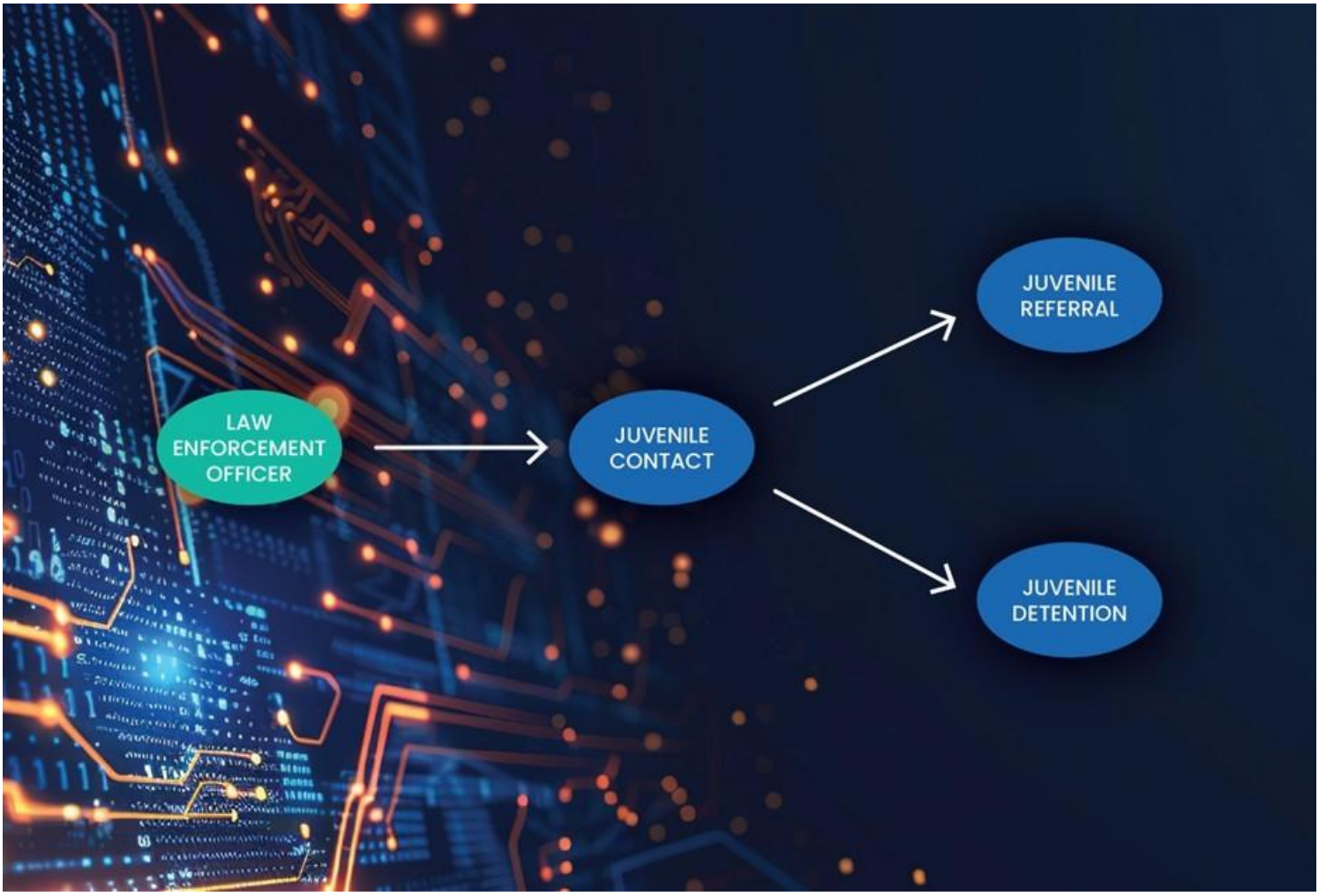
9.4 DUI ARREST

Driving under the influence (DUI) of drugs or alcohol, or while impaired in any other way, is a serious public safety concern in traffic enforcement. A DUI investigation may begin during a routine traffic stop or in response to an accident. If a law enforcement officer suspects impairment, field sobriety tests may be conducted when it is safe to do so, followed by a chemical test in the field or under controlled conditions. The officer must ask the subject if they are willing to submit to a chemical test, and the response should be documented in the RMS. In fatal cases, officers may be required to obtain a chemical test without the subject's consent. If a test is not performed due to refusal or safety concerns, this must also be documented per department policy. All relevant test results should be recorded in the RMS to supplement the report. Although some states may have a specific DUI required form, it should be noted that the DUI should also be documented in the RMS as it is a NIBRS reportable arrest.

The department's SOP for DUI arrests should be followed, with each step documented in the RMS. Evidence collected from these incidents must be properly handled and tracked. In some cases, a DUI arrest may require a Complaint for a Search Warrant, particularly for chemical testing when consent is refused. The RMS should support or integrate with the Jail Management System (JMS) to facilitate this process efficiently and ensure that any Complaint or Search Warrant is attached to the incident report. Additionally, DUI search warrants and related policies should be incorporated into the documentation to ensure compliance with legal and procedural requirements.

CHAPTER 10 | JUVENILE CONTACT

10.1 JUVENILE CONTACT DIAGRAM



The juvenile justice system requires special handling of information about juveniles. Paramount is the handling of their records, which must conform to state and federal legal requirements that specifically define privacy protections. Regulations for the handling of juveniles vary from state to state. These rules must be implemented based on 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. 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, on certain activities involving juveniles.

The RMS should be able 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).

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

10.2 JUVENILE CONTACT

Contact with a juvenile should be documented in the RMS, as it may result in a citation, referral, or detention. Taking a juvenile into custody allows a law enforcement officer to assess their situation and ensure their safety. The officer will gather information about the incident to determine whether a criminal offense or status offense occurred and whether any sanctions are necessary.

In some jurisdictions, juveniles taken into custody are brought to a juvenile intake center for assessment, while in others, qualified personnel within the law enforcement agency conduct the evaluation. If the circumstances require a more serious response than an admonishment, the officer will determine the appropriate course of action based on factors such as the nature of the incident, the presence of weapons or narcotics, prior law enforcement contacts, and whether victims are involved. In many jurisdictions, referral to juvenile intake is required if a pattern of delinquency exists within a legally defined timeframe.

A juvenile may be released to a parent, guardian, hospital, or non-judicial authority. In some cases, informal diversion programs, such as requiring community service, may be used. The RMS should provide a mechanism for timed alert notifications if follow-up contact or additional information is needed.

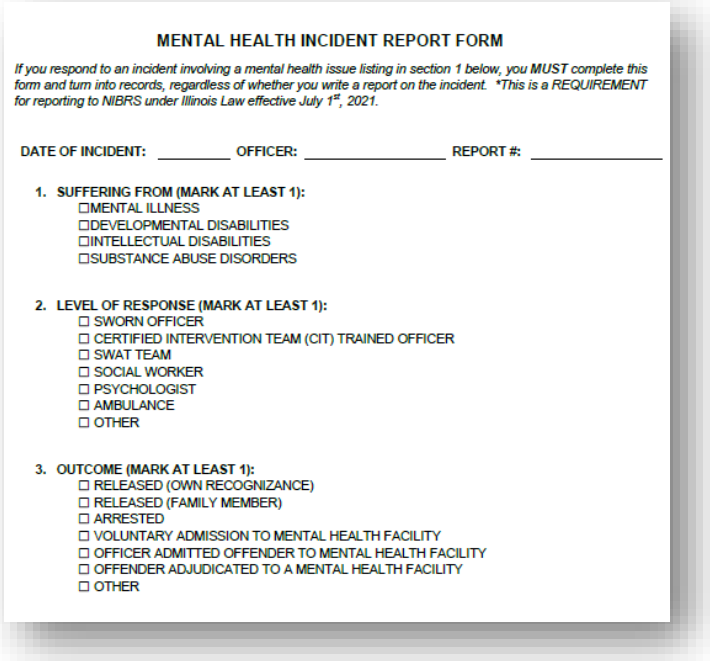
The RMS will support these processes by documenting all interactions with the juvenile in a juvenile contact record and guiding the officer toward the appropriate remedy, sanction, or referral based on the circumstances. Law enforcement officers must also coordinate with professionals conducting the investigation and communicate with the juvenile's parents or guardians. These contacts, along with details such as the juvenile's full name, age, address, family and associate information, gang affiliations, physical description, gender, school name, contact details (cell phone and email), and incident-related information, should be recorded in the RMS to ensure comprehensive documentation.

10.3 JUVENILE DETENTION

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

10.4 JUVENILE REFERRAL

Formal charges may be filed against the juvenile, or they may be released to a parent or guardian, a hospital, or another non-judicial authority. In some cases, informal diversion programs may be used, such as assigning community service. The RMS should provide a mechanism for follow-up notifications, either through timed alerts or reports, to ensure necessary actions are taken. Juvenile diversion tracking may be incorporated to monitor program outcomes and success. If mental health services are involved and related information is recorded in the RMS, policies must be in place to regulate the sharing and access of this sensitive information.



MENTAL HEALTH INCIDENT REPORT FORM

*If you respond to an incident involving a mental health issue listing in section 1 below, you MUST complete this form and turn into records, regardless of whether you write a report on the incident. *This is a REQUIREMENT for reporting to NIBRS under Illinois Law effective July 1st, 2021.*

DATE OF INCIDENT: _____ OFFICER: _____ REPORT #: _____

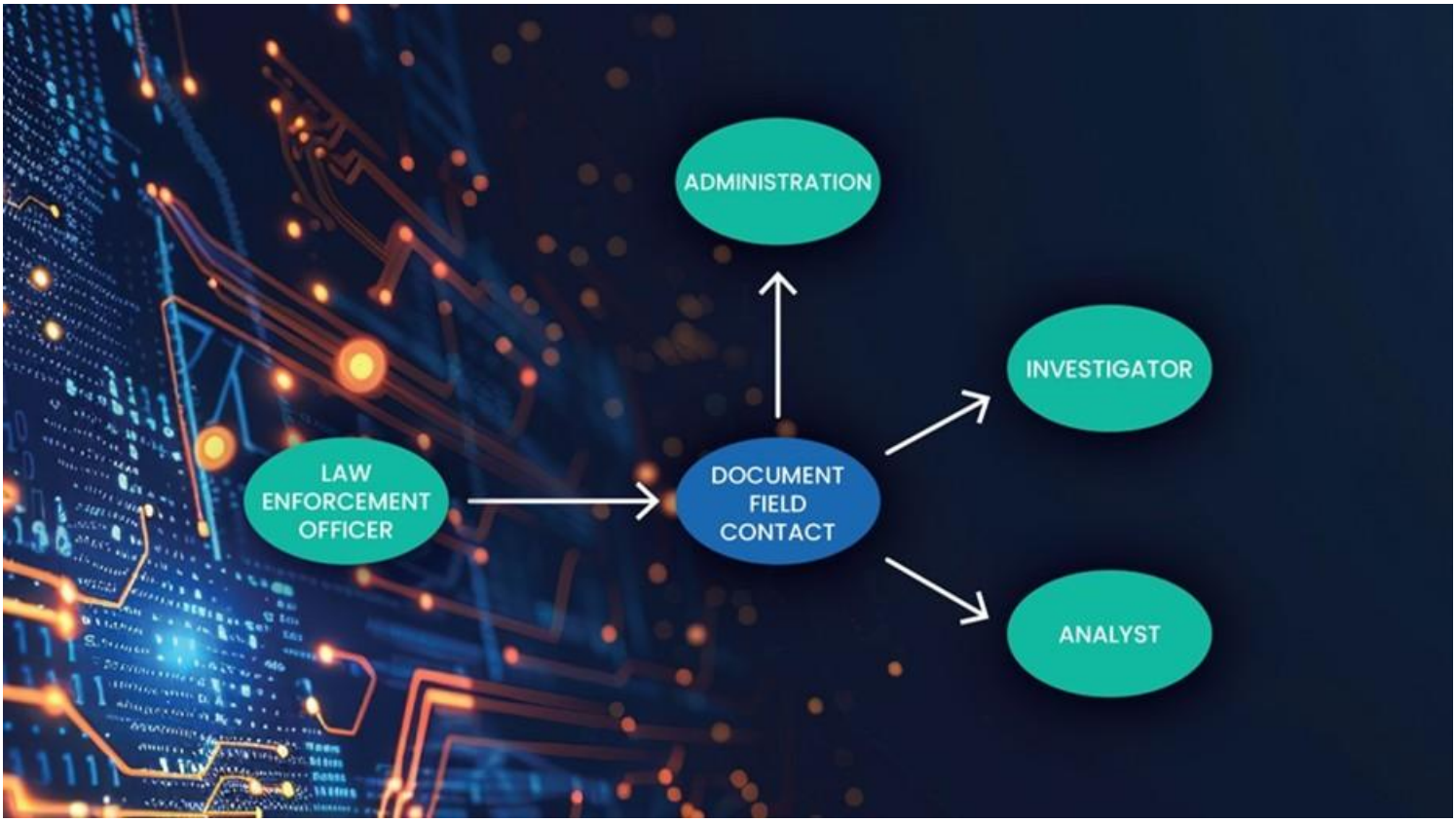
1. SUFFERING FROM (MARK AT LEAST 1):
   - ☐MENTAL ILLNESS
   - ☐DEVELOPMENTAL DISABILITIES
   - ☐INTELLECTUAL DISABILITIES
   - ☐SUBSTANCE ABUSE DISORDERS

2. LEVEL OF RESPONSE (MARK AT LEAST 1):
   - ☐ SWORN OFFICER
   - ☐ CERTIFIED INTERVENTION TEAM (CIT) TRAINED OFFICER
   - ☐ SWAT TEAM
   - ☐ SOCIAL WORKER
   - ☐ PSYCHOLOGIST
   - ☐ AMBULANCE
   - ☐ OTHER

3. OUTCOME (MARK AT LEAST 1):
   - ☐ RELEASED (OWN RECOGNIZANCE)
   - ☐ RELEASED (FAMILY MEMBER)
   - ☐ ARRESTED
   - ☐ VOLUNTARY ADMISSION TO MENTAL HEALTH FACILITY
   - ☐ OFFICER ADMITTED OFFENDER TO MENTAL HEALTH FACILITY
   - ☐ OFFENDER ADJUDICATED TO A MENTAL HEALTH FACILITY
   - ☐ OTHER

CHAPTER 11 | FIELD CONTACT

11.1 DOCUMENT FIELD CONTACT



A field contact record is created by a law enforcement officer in accordance with the department's SOP. This process is typically initiated by unusual or suspicious circumstances or any activity deemed noteworthy by the officer that would not otherwise be documented in the RMS (refer to the Incident Reporting module for more details).

Data recorded in the Field Contact module is available for analytical support, including crime analysis, and can be searched by investigators to develop leads. Unlike incident reports, field contacts do not require the same level of review and approval.

The module should enable officers to collect demographic data on individuals involved for statistical reporting in bias-based policing programs. Additionally, the system should support the automatic transmission of 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 federal information-sharing systems (e.g., RISS, ARJIS, LInX, OHLEG, N-DEx, ISE)
- Mug shot repository
- Electronic Fingerprinting Device
- Mobile computing system

Standard Internal Data Exchanges:

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

11.2 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 or in potentially sensitive areas, such as areas near schools and religious institutions. The information collected includes:

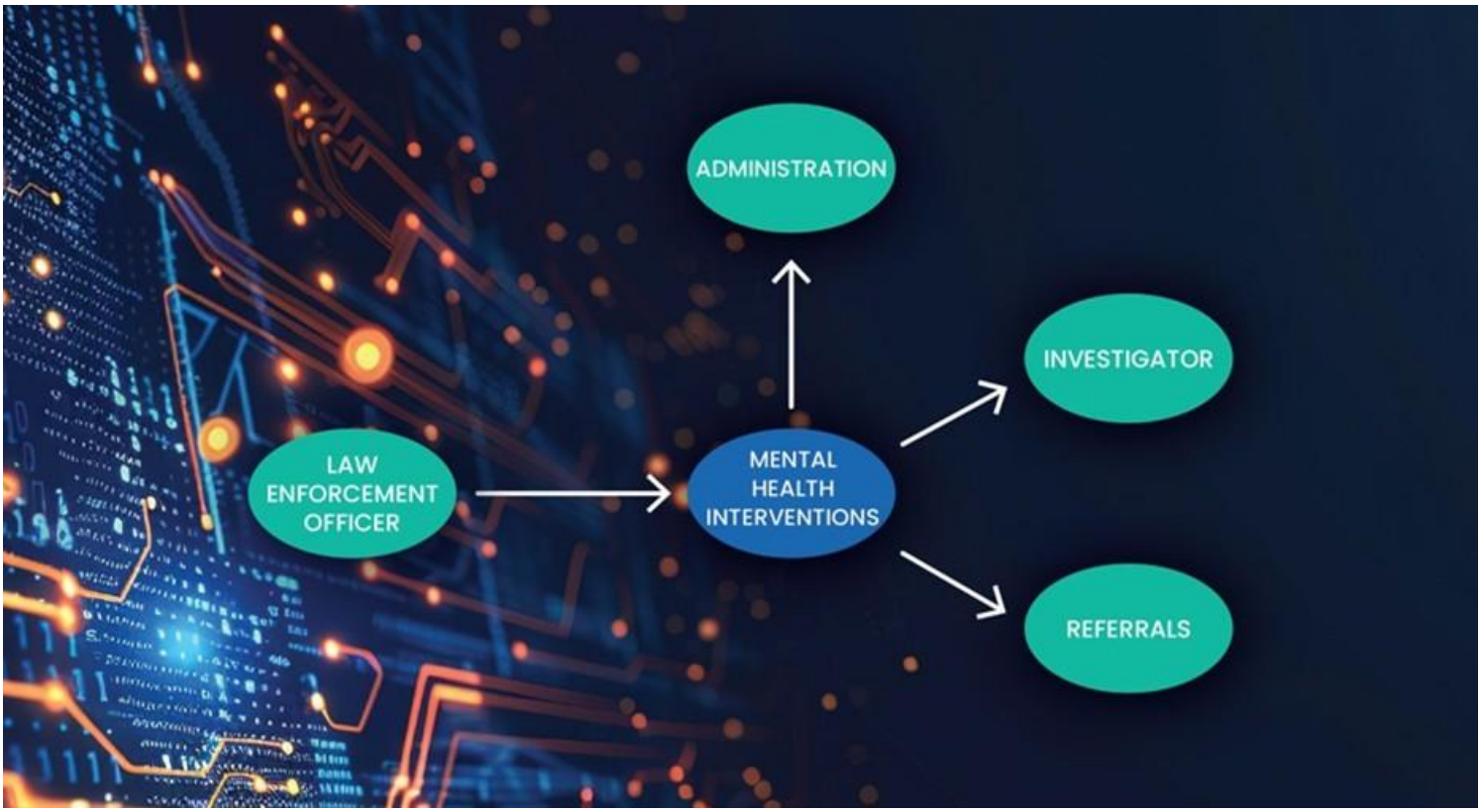
- Location and time
- General circumstances
- Names and descriptions of people involved
- Identifying information on vehicles or other property
- Photographs and other electronic attachments

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

Unlike incident reports, field contact reports are usually not subject to a stringent supervisor review and approval process. However, they are reviewed to ensure the quality and adequacy of reporting and consistency with departmental policy and statute.

CHAPTER 12 | MENTAL HEALTH INTERVENTIONS

12.1 MENTAL HEALTH INTERVENTIONS DIAGRAM



While there may not be a separate module specifically dedicated to mental health interventions in all systems, this topic is included due to the increasing frequency and relevance of mental health crises within law enforcement encounters. As these incidents become more common, public safety agencies must have clear guidelines for documenting and managing mental health-related interactions to ensure appropriate follow-up and coordination with health professionals.

Mental health interventions should generally be documented using the incident report or field contact record module, depending on the nature and severity of the interaction. Some agencies may prefer using the incident report module to ensure better tracking, awareness, and appropriate follow-up. Incident reports provide a more structured and detailed record of interactions, particularly those requiring future intervention, resource allocation, or legal considerations. These reports ensure that mental health-related incidents are properly documented for ongoing case management, risk evaluation, and future law enforcement or health interventions.

In cases where the interaction does not rise to the level of an incident requiring a full report but still involves concerns about an individual's mental health (e.g., welfare checks or encounters with individuals in crisis without criminal activity), it may be useful to document key details in the field contact record module. This module captures essential information while providing flexibility when a full incident report is not warranted, ensuring that officers can easily reference past interactions if needed.

Agencies should establish clear guidelines for when to use the incident report module versus the field contact record module for mental health interventions. This includes documenting the nature of the mental health crisis, the response provided by law enforcement, any resources or referrals (e.g., mental health services, emergency psychiatric care), and the involvement of specialized units such as Crisis Intervention Teams (CIT).

By properly documenting mental health interventions through the appropriate module, law enforcement agencies can improve their response to individuals in crisis, ensure comprehensive care coordination, and facilitate better communication with mental health professionals and other relevant community stakeholders.

CHAPTER 13 | ANALYTICAL SUPPORT

13.1 ANALYTICAL SUPPORT DIAGRAM

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 the analyst uses by providing read access to all data included in the RMS or replicating the data in a server used for analytics. In this case, the frequency for refreshing this data must be clearly defined to facilitate custom queries or data ingestion into analytical tools. The agency should also require access to the RMS data dictionary, including the relational schema, to ensure a clear understanding of the data.

Analytical tools have matured significantly, allowing agencies to develop dashboards that 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 the layering of other data sets and should be able to gather new maps/layers to get updates from the source data. The RMS should include user-friendly descriptions of the reporting methodology to clearly describe the data output (i.e. if reporting crimes vs. persons, does the report include the National Incident-Based Reporting System (NIBRS) methodology of counting the number of victims for crimes against persons, or is the report counting the number of offenses?).

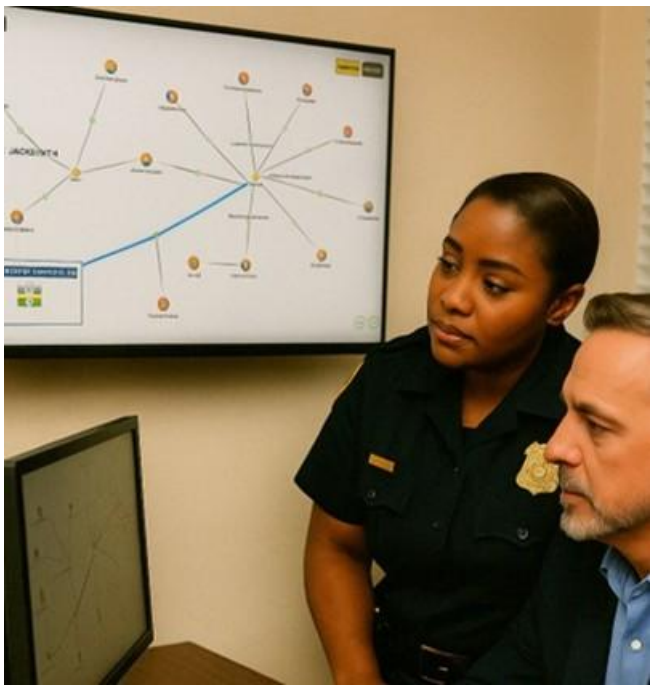
Analytical support can be subdivided into four main types:

1. **Administrative/Operational Analysis:** Provides information to support command-level decision-making, including resource allocation, staffing, policy development, and budget planning.
2. **Tactical Analysis**: Provides timely, actionable information to assist officers and investigators in identifying specific, immediate policing problems and arresting criminal offenders.
3. **Strategic Analysis:** Provides information concerning long-range crime problems and underlying issues to

inform agency-wide planning, crime prevention initiatives, and proactive policing strategies.

4. **Intelligence (or Investigative) Analysis**: Supports investigations by analyzing data on suspects, criminal organizations, or events to identify relationships, predict behavior, and guide enforcement actions.

In addition to querying and producing 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 for specified time periods. The analyst should be able to define the time period, whether it is the last 30 days, the last six months, the last fiscal year, or the 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, and spatial and temporal tools. The results of these analyses should be stored in the RMS for a time determined by the jurisdiction's SOP. They can be used to assess agency performance and support administrative decisions. The RMS should have a variety of reporting functions attached to its Analytical Support modules and allow the 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 one or more criteria, including:

- Geographic area, beat, or reporting district (e.g., ZIP codes)
- Date, time, and day of week
- Frequency of occurrence
- Citation type
- Crime or incident report type
- Field interview type
- Warrant type
- Property and vehicle information type
- Offense category (e.g., disorder, property crime, violent crime)
- Crime target type (e.g., person, residence, vehicle, business)

The system should also 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 using query interfaces that are part of the application or, at a minimum, 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 related to time, such as the day, time of day, week, date, month, and year. It should also 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 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
- Stolen Property

Standard External Data Exchanges:

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

13.2 ADMINISTRATIVE AND OPERATIONAL ANALYSIS

Administrative and operational analysis supports internal decision-making and external reporting by providing both high-level statistical summaries and evaluations of agency performance. Administrative analysis typically focuses on long-range, strategic reporting, such as quarterly or annual summaries, used to inform executive leadership, oversight bodies, neighborhood groups, and the public. It may incorporate economic, geographic, and crime-related data to support transparency and long-term planning. On the other hand, operational analysis focuses on evaluating internal processes, resource allocation, workload distribution, and performance metrics to improve efficiency and effectiveness.

Where required by the agency's standard operating procedures, the RMS should support the ability to generate statistical reports on all law enforcement activities, allocate costs to those activities, and track performance measures defined by the agency. Administrative and operational analysis provides a foundation for informed policy decisions, strategic planning, and resource management.

13.3 TACTICAL ANALYSIS

Tactical analysis provides timely, actionable information to assist law enforcement personnel, such as patrol and investigative officers, in identifying specific and immediate crime or disorder problems, disrupting criminal behavior, and facilitating the arrest of offenders. This type of analysis is geared toward short-term response and requires rapid access to accurate data to support decision-making in the field. Analytical insights are used to detect crime patterns, identify emerging hotspots, and coordinate operational responses.

To support effective tactical analysis, the RMS should facilitate the timely entry, review, approval, and dissemination of relevant data. The system must also include safeguards to ensure data quality and validation, minimize reporting delays, and enhance the reliability of the information used to guide real-time enforcement actions.

13.4 STRATEGIC ANALYSIS

Strategic analysis focuses on identifying and understanding long-term crime patterns, systemic issues, and organizational challenges to support more effective and efficient fulfillment of the agency's mission. It is primarily concerned with developing solutions to ongoing or recurring problems, often using aggregated data to uncover underlying causes and assessing the impact of social, economic, or environmental factors. This form of analysis contributes to long-range planning, resource deployment, crime prevention initiatives, and policy development.

Strategic analysis may also involve elements of business intelligence, helping agency leadership make informed decisions through data-driven insights. To support this function, the RMS should allow for comprehensive trend analysis, historical comparisons, and the ability to merge various data sources for deeper understanding and long-term forecasting.

13.5 INTELLIGENCE/INVESTIGATIVE ANALYSIS

Intelligence/investigative analysis supports investigations by analyzing data related to suspects, criminal networks, and events to uncover patterns, identify relationships, predict behavior, and inform enforcement strategies. Forecasting within intelligence analysis can help anticipate shifts in

criminal activity following the disruption of a network or operation, allowing agencies to prepare for potential displacement or changes in offender behavior proactively.

13.6 FORECASTING ACROSS CRIME ANALYSIS FUNCTIONS

Forecasting is not typically viewed as a standalone type of crime analysis but rather a cross-functional capability that enhances all forms of analysis: administrative, tactical, strategic, intelligence, and operational. It involves using historical data, current trends, and contextual information to project future events or conditions, enabling law enforcement agencies to take preemptive and proactive measures.

In administrative and operational analysis, forecasting helps agencies anticipate future resource needs, staffing changes, and budget requirements based on projected call volumes, population growth, or officer attrition. This allows agencies to plan effectively and align resources with anticipated demands.

In tactical analysis, forecasting supports short-term crime suppression efforts by helping identify when and where future incidents in a crime series are likely to occur. This enables agencies to deploy resources strategically and intervene before additional crimes occur.

In strategic analysis, forecasting can inform long-term planning by identifying how broader trends, such as demographic shifts, urban development, or social changes, may influence crime patterns over time. These insights help agencies design forward-looking prevention strategies and allocate resources more efficiently.

In intelligence (or investigative) analysis, forecasting enables investigators to assess how dismantling a criminal organization or arresting a key offender may impact future criminal activity. It can also help predict retaliatory acts, emerging threats, or shifts in criminal networks, allowing for more focused enforcement and monitoring.

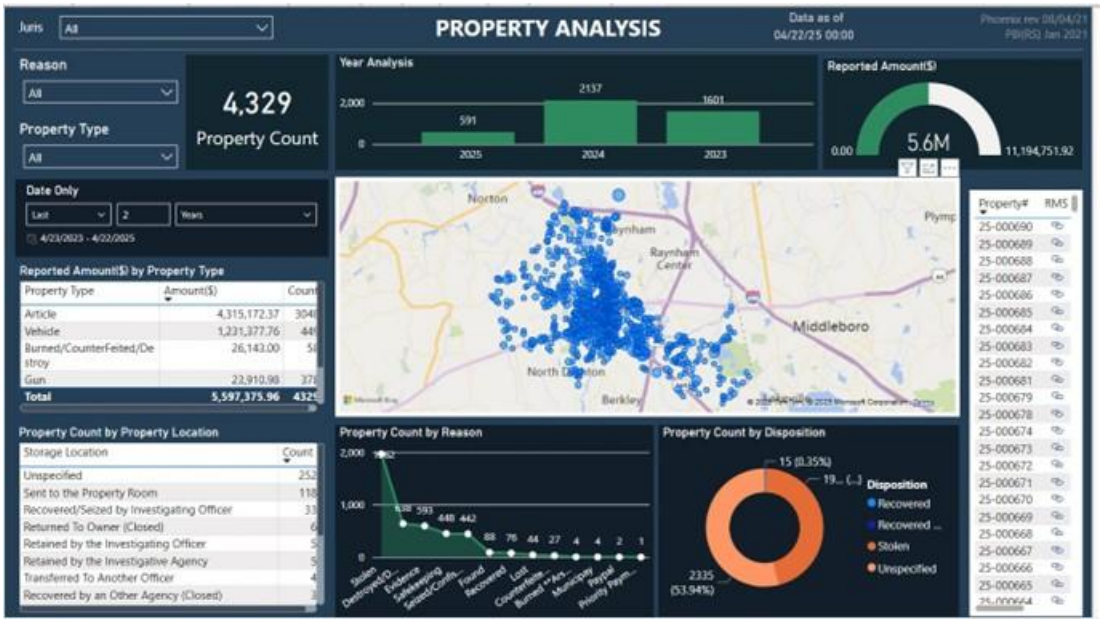
By integrating forecasting into all analytical functions, agencies can improve investigative outcomes, reduce response times, allocate resources more effectively, and ultimately enhance public safety. RMS and analytical systems that support forecasting capabilities through historical data analysis, trend modeling, and scenario planning offer agencies a critical tool to stay ahead of evolving crime challenges and operational needs.

13.7 REPORT OUTPUT

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

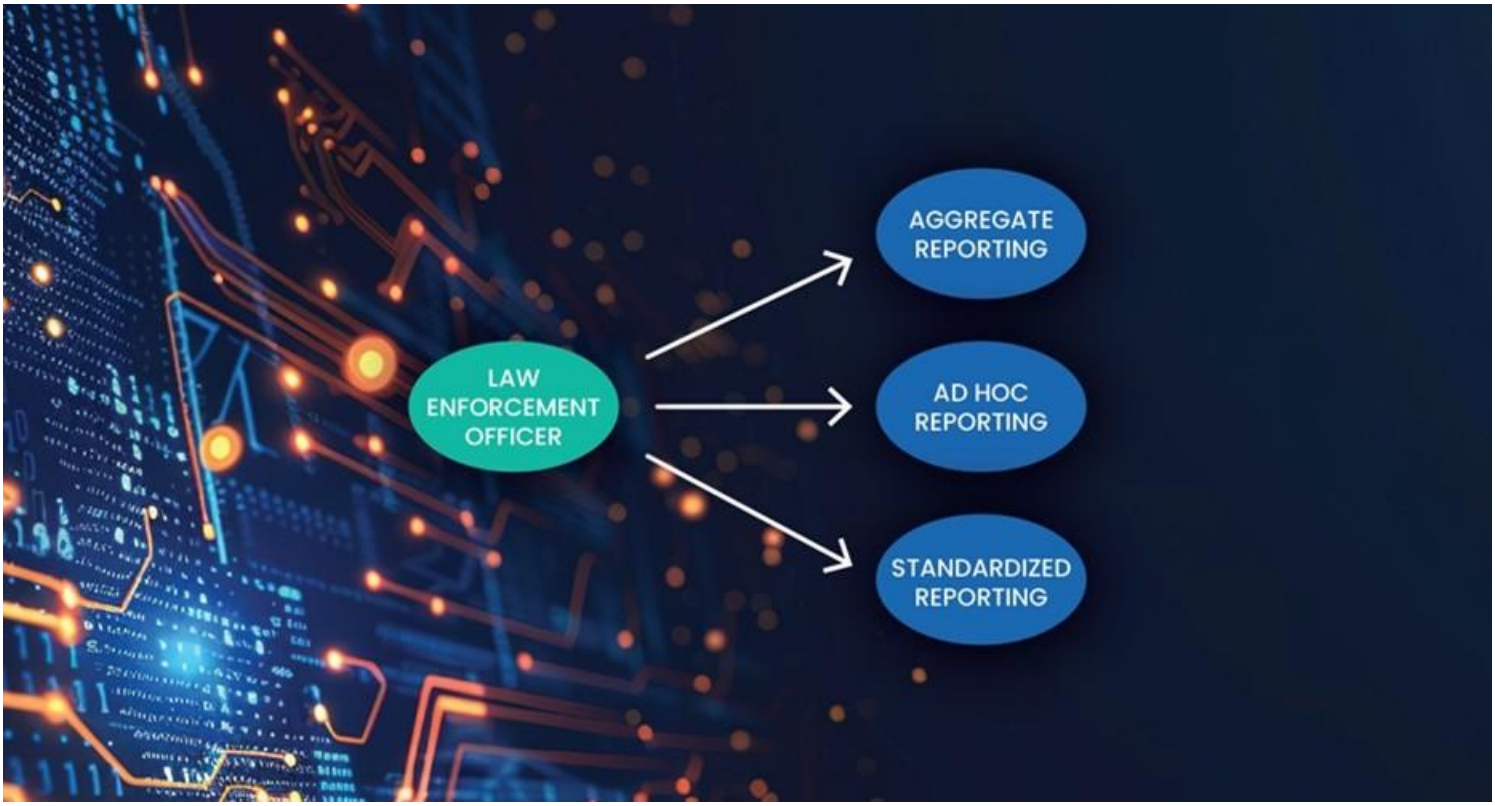
13.8 CRIME MAPPING/DASHBOARDS

Crime mapping and dashboards are now widely used in law enforcement for data-driven decision-making in evaluating patterns and trends, crime incidents/rates, hotspots of crime or calls for service, the deployment of resources, and expenditures, among others. The RMS may allow the agency to create customized dashboards using live data that allow for multiple filters across multiple tables, with various display options such as graphs, charts, and maps, including incident and density maps. If agencies use third-party products to conduct crime mapping and to create dashboards, the RMS should have the capability for authorized users to export data and/or connect to the RMS database via open database connectivity (ODBC) protocols to allow access to necessary fields, such as address, latitude/longitude, offense or activity type, and/or integrate with necessary CAD data, e.g., type of call, duration of call, and number of officers assigned to a call.



CHAPTER 14 | RMS REPORTS

14.1 RMS REPORTS DIAGRAM



Robust reporting is a core requirement of an RMS. The law enforcement agency enters data into the solution for 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 generated in the course of routine police operations (e.g., arrest reports and incident reports). Aggregated reports are developed by line and supervisory staff and reviewed by law enforcement executives. Role-based security should restrict access to some reports. The RMS should include user-friendly descriptions of the reporting methodology to describe the data output clearly.

Law enforcement personnel must be able to generate standardized and aggregate reports and 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, which allows the law enforcement agency to generate customized reports to meet their exact needs. Typically, third-party products are used for ad hoc queries and reports.

Standard output reports for the RMS business functions are:

- Incident reports
- Arrest reports
- Use of Force reports
- Crash reports
- Property/evidence reports
- Citation reports
- Field interview reports
- Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS) reports
- Case management reports
- Billing reports
- Summary reports for warrants, citations, CFS, collisions, and employees

14.2 AGGREGATE REPORTING

Aggregate, agency-wide reporting allows law enforcement personnel to associate information in a variety of ways and among several different tables or fields, including calls for service, warrants, incident reports, arrest reports, collision data, property data, and weapons data.

Users must be able to query, retrieve, and display information in a variety of ways. They must be able to query indicators, such as the 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, group of passwords, or role.

14.3 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 be able to redact public reports and save a copy of the redacted report. The RMS should also include the ability to electronically save copies of reports for sharing with key external stakeholders.

14.4 STANDARDIZED REPORTING

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

14.5 AD HOC REPORTING

The agency may need operational reports and analyses that are not provided by standard RMS reports and queries. Ad hoc reporting will allow users 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. A third-party solution may provide this ad hoc reporting tool or mechanism. This solution may be embedded in the application or run as a stand-alone function. Ad hoc reporting functions 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 standalone 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 access the data without compromising RMS security controls and performance.

14.6 DATA QUERIES

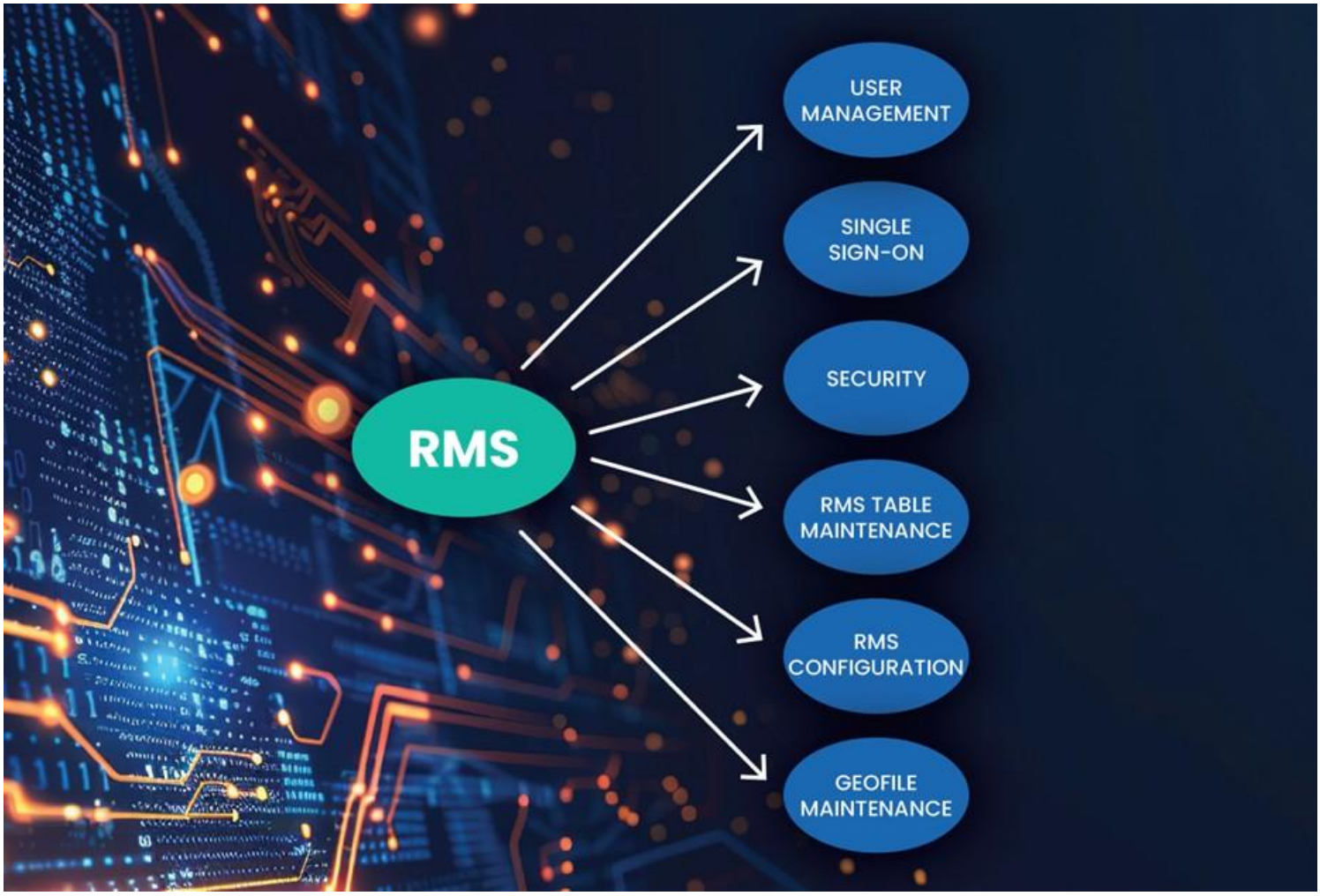
Individuals at all levels of the law enforcement agency should be able to perform ad hoc data queries based on permission. These queries should allow the agency to search for all data elements in the solution. The RMS should enable the user to cascade searches to refine information of interest. The RMS should also provide the ability to search all narrative fields. The RMS should support configurable dashboards and real-time data visualization to enhance decision-making. The RMS should be equipped to handle granular permissions regarding the generation of these data queries based on user permissions.

14.7 CLERY ACT

Colleges and Universities are required to report Campus Crime Statistics under the Clery Act. This reporting does not replace the reporting of NIBRS statistics to the FBI. The RMS should have the capability to produce reports for offenses related to dating violence, domestic violence, sexual assault, and stalking, along with the data elements required under the Clery Act. Refer to the 2016 Clery manual for more information.

CHAPTER 15 | RMS SYSTEM ADMINISTRATION

15.1 RMS SYSTEM ADMINISTRATION DIAGRAM



Many aspects of an RMS should be configurable to meet specific agency requirements. The RMS administration functions address these aspects. Configurable aspects may include roles and security, domain values, use of incident and case number formatting, supplements, and approval workflows. 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 create and query information effectively, ensure appropriate access to information and system security, and ensure effective departmental information.

Example administrative functions include:

- RMS user management
- Single sign-on
- Security
- RMS table maintenance
- RMS configurations (e.g., parameters, defaults)
- Geofile maintenance

Standard Outputs:

- Report on users, sortable by name, access level, password age, and machine used
- Report on RMS use, sortable by user log-in, frequency, total time in system, number of concurrent logins, machine used, and duration time-outs
- Report on failed logins, 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

15.2 USER MANAGEMENT

The RMS must provide comprehensive tools to manage user accounts, roles, and access privileges across the system. User management is essential to ensuring that only authorized personnel have access to appropriate information and system functions, based on their job responsibilities.

The system should support centralized administration of user accounts, including the ability to create, modify, deactivate, and delete users. Role-based access controls should be used to assign permissions at a granular level, ensuring that users can only view or modify the data necessary for their function. These roles should be configurable and support various levels of access based on agency-defined criteria, such as rank, assignment, or division.

User management should also include the ability to:

- Assign users to one or more roles or groups
- Configure permissions by module, function, or data element
- Apply access restrictions for sensitive data (e.g., confidential informants, internal investigations)
- Enforce password complexity rules and expiration policies
- Track password age and login history for auditing purposes
- Support user-specific settings such as preferred time zones or dashboard layouts

In multi-jurisdictional or regional deployments, the RMS should allow administrators to control user access across agency boundaries while maintaining agency-specific security settings and workflows. The system should also support integration with agency directory services (e.g., Active Directory) to streamline account creation and authentication, and to facilitate automatic provisioning and deactivation in line with agency onboarding or offboarding processes.

To maintain system integrity and security, all changes to user roles or permissions should be logged in the audit trail and made visible to administrators through reporting and notification tools.

15.3 SINGLE SIGN-ON

Many organizations utilize secure external directory services to manage access across agency applications. The RMS should support integration, enabling users to sign on once and gain access to all authorized applications without requiring multiple logins. Advanced authentication methods, including access through the agency's Virtual Private Network (VPN), should be supported to enhance security and streamline access.

All authentication methods must comply with encryption requirements outlined in security policies to protect user credentials. Additionally, the RMS should align with FBI CJIS Security Policy requirements for multi-factor authentication (MFA) to ensure compliance with federal guidelines for accessing criminal justice information. Implementing these security measures reduces the need for users to remember multiple usernames and passwords while maintaining a high level of data protection.

15.4 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 exist for identification technologies, such as identification cards and security tokens. Multi-factor authentication should follow the latest version of the FBI CJIS Security and NIST[ii] Policies.

Security groups are often assigned based on 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 be able to grant access to the individual user level for certain modules such as Case Management and Confidential Informants. In addition, the solution should include the ability to integrate with an agency's existing user management solution, such as to control permission changes (add/edit/delete) in a centralized fashion if the agency is equipped to do so.

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 consider local, county, state, and national security policies and requirements (e.g., CJIS security policy).

15.5 RMS TABLE MAINTENANCE

The RMS should allow the user agency to define and maintain code lists and associated literals (i.e., plain English translations) 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 NIEMOpen, NIBRS, and NCIC. If the law enforcement agency chooses to expand standard code tables such as location types, it must ensure the RMS can provide a crosswalk to the appropriate NIBRS, NIEMOpen, or NCIC codes. 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.

15.6 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, agency logo, 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 an adequate warning to prevent inadvertent damage to the system.

15.7 GEOFILE MAINTENANCE

The geofile (the master location file) is used to validate and standardize location and address information, ensuring that addresses are accurately represented within the system. It is also employed 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 data to confirm the validity of an address, making it a critical tool for accurate record-keeping and location-based analysis.

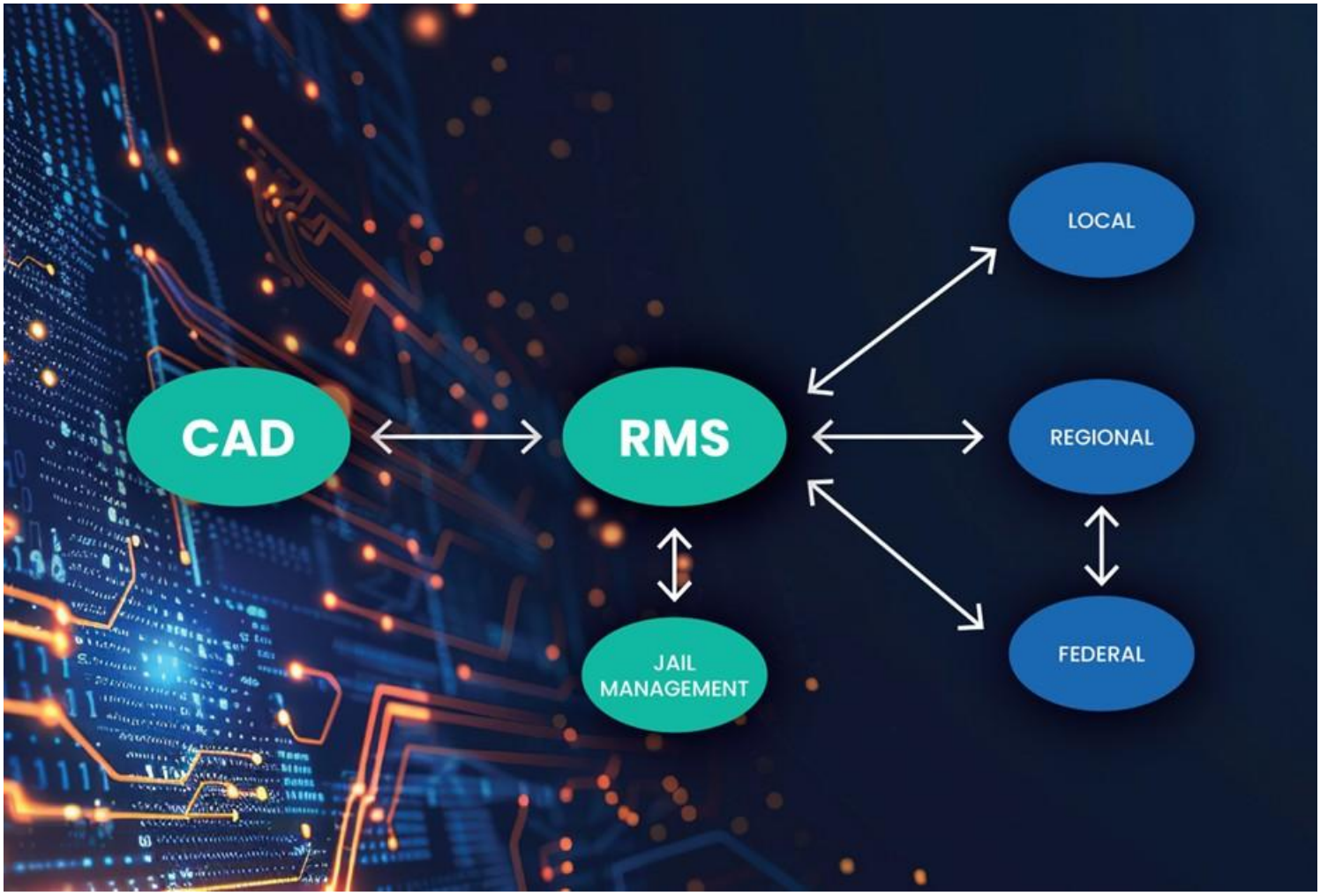
In addition to basic address validation, the geofile enriches data with location-based information, enabling the system to analyze and represent geographic patterns, relationships, and spatial contexts. It cross-references addresses and locations using common names (e.g., business names, parks, hospitals, and schools) and street aliases, providing valuable geographic context for law enforcement operations. All addresses in the RMS are assumed to be validated using this system geofile.

Geofiles can be populated with data from various sources, including CAD data spills or integration with external systems such as Google Maps/Places. These integrations improve the accuracy and timeliness of the geofile, ensuring that location data remains consistent across systems. This validation helps maintain the integrity of geographic data, which is critical for effective decision-making and operations.

Geo-verified data plays a key role in crime mapping and data analysis by linking criminal activity to specific geographic locations. This enables agencies to visualize crime patterns, identify hotspots, and deploy resources more efficiently. Geo-verified data also supports proactive policing by analyzing trends in crime distribution and helping agencies anticipate and prevent future incidents. The system must provide an agency with the ability to input and update all geofile data, including the physical address and latitude/longitude/altitude coordinates, to maintain the most accurate and up-to-date information.

CHAPTER 16 | RMS INTERFACES

16.1 RMS INTERFACES DIAGRAM



As law enforcement requirements 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. Local business practices and local agency workflows will largely determine the exact nature of those exchanges. All interfaces need to comply with state and national requirements and standards. Each business function described in this document includes examples of data exchanges. Interfaces should be based on open standards and be repeatable across multiple agencies. The NIEMOpen should be utilized, when possible, to exchange data between systems. The RMS and agency should refer to this standard's most recently published version.

Sections 16.4 and 16.5 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 systems, human resources systems, state systems, and multi-jurisdictional information systems. The RMS should also interface with the citizen reporting tool utilized by the agency. These interfaces should be based on national standards, such as NIEMOpen, NIBRS, and NCIC.

16.2 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 people, 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 and wanted people, 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 with multiple systems, including gunshot and other locator systems, gang tracking systems, mapping technology, ballistics tracking, automatic portable radio identification, and others.

16.3 JAIL MANAGEMENT INTERFACES

When a subject is arrested, information may be transferred from the RMS to a county or regional jail management system. Integrating these systems ensures that data collected during the incident, investigation, and arrest are transferred to the jail management system.

Inmate information about arrested individuals is transferred from the RMS to the JMS, including personal details, charges, and booking information. The arrest report, including the arresting officer's details, may also be sent to the JMS when the arrestee is booked into the jail. Information on pre-existing medical conditions, prior law enforcement encounters with the arrestee, and data regarding scheduled court dates, hearing outcomes, and court orders can also be transferred from the RMS to the JMS for tracking.

The JMS can transfer changes in arrest statuses, such as dismissals or modifications, to the RMS. The JMS can also share updates on inmate court appearances and results of legal proceedings, including court disposition. Updates on holds or the status of warrants may be communicated to the RMS. Finally, details on inmate releases, parole eligibility, and conditions may be sent to the RMS for tracking and compliance.

The RMS/JMS interface will reduce redundant entry and allow jail and law enforcement staff to collaborate to improve workflow and response times.

16.4 LOCAL/REGIONAL INTERFACES

The RMS must be able 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 vehicles, property and evidence, pawn shops, third-party pawn applications, gang tracking, citizen reporting, permits and licenses, and laboratory management systems. Where possible, NIEMOpen standards should be used to develop 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 of 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.

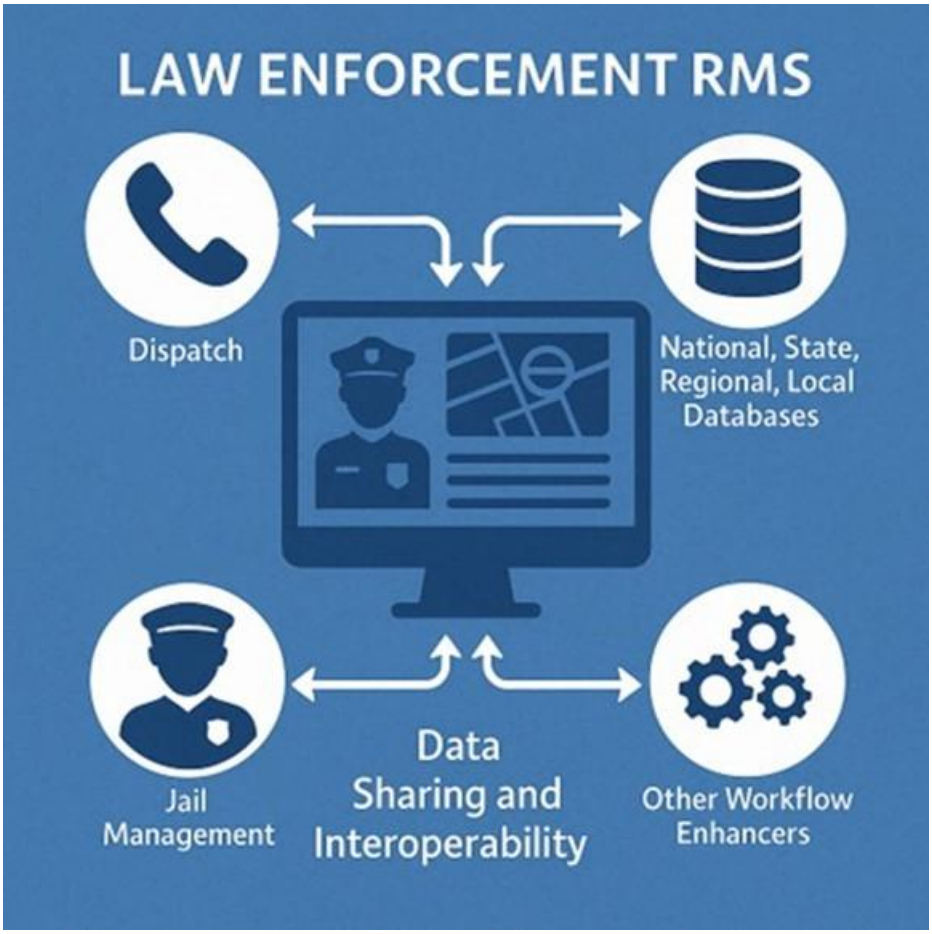
16.5 STATE/FEDERAL INTERFACES

The RMS needs to interface with state and federal information-sharing systems. In some cases, the state and federal interfaces are facilitated through a county for state interfaces or a regional or state interface for federal information-sharing. State interfaces may include traffic citations, collision reporting, and NIBRS. OHLEG, RISS, ISE, and State Fusion Centers provide other examples of systems that the RMS may interface with. Many law enforcement agencies send data to the FBI's N-DEx system directly or through a regional system such as LInX or a state information-sharing system. While it is more common for law enforcement agencies to interface with NCIC or Nlets from their CAD system, some RMS solutions do interface with these solutions via their county or state switches. These interfaces should be based on national standards such as NIEMOpen and NCIC, where possible. Agencies reporting NIBRS must adhere to their state specifications. Some interfaces will merely involve the development of a web service to push and/or 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 systems will improve officer efficiency 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 CFS, incident, arrest, collision, citation, and booking data for investigative purposes. N-DEx submissions are based upon the NIEMOpen standard. The most current versions of these standards should be used for implementation. It should be noted that agencies may send data to N-DEx via a regional or state information sharing system such as LInX or ARJIS.

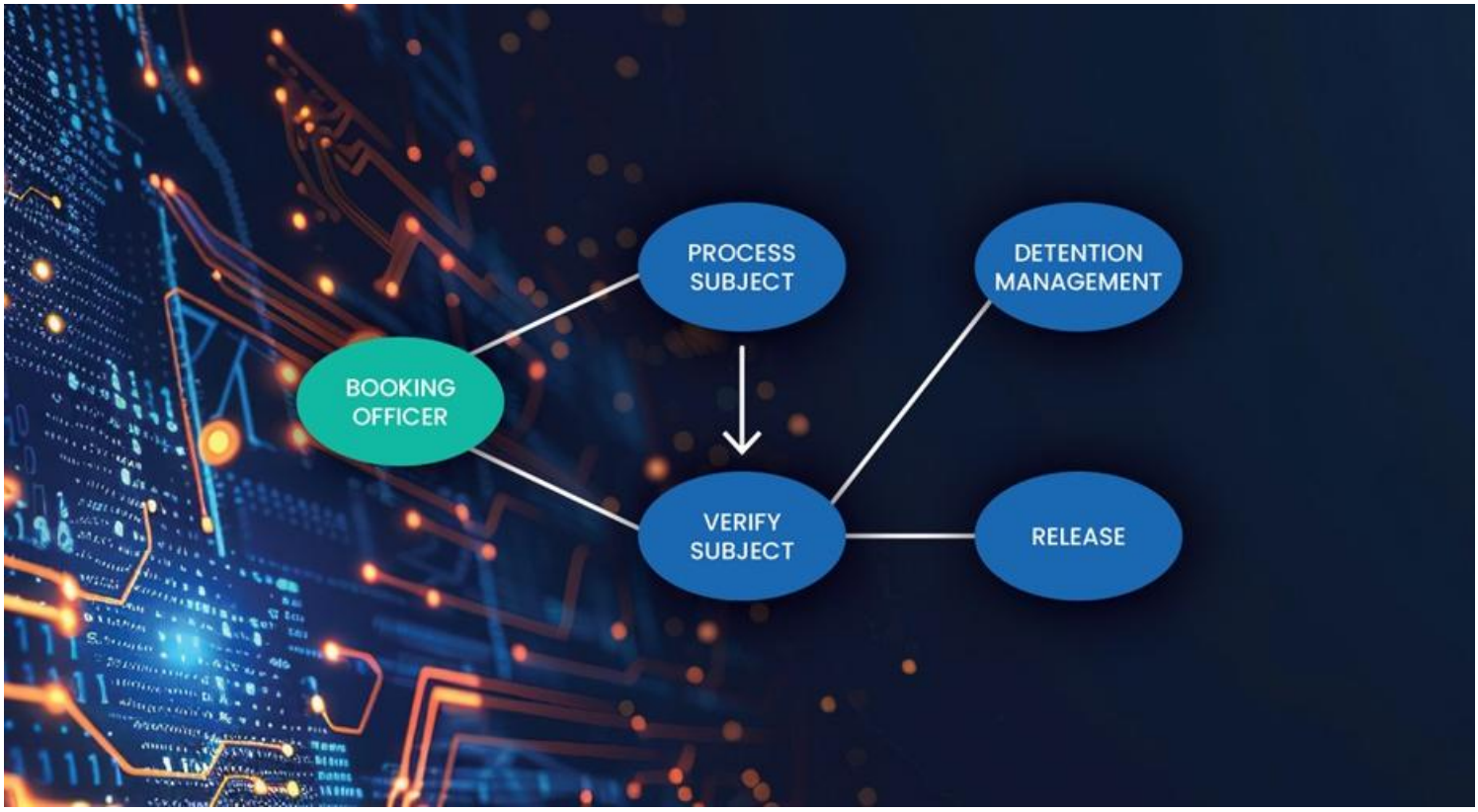
When interfacing with local/regional or state/federal systems, consideration should be given to the analytical or investigative needs of the external agency accessing the data. For example, the State on a call for service may be assumed by the agency but unknown by an external agency and should be included in the export.

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 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 and all other crimes.



CHAPTER 17 | BOOKING

17.1 BOOKING DIAGRAM



Booking data captured in a law enforcement RMS is ultimately linked to the arrest report. The data to be captured includes the subject's personal information and the official charges for which the subject was arrested. After completing 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 later.

The personal identification information provided by the subject will be checked against the Master Name Index to create a link to the booking record and avoid unnecessary or redundant data entry. Personal information includes the subject's name and any known aliases; a physical description, including scars, marks, 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 of the subject will also be taken and may include images of any identifying attributes, such as scars, marks, and tattoos. The RMS will provide the capability to store the images in the database linked to the booking record.

Standard Outputs:

- Booking form
- Booking summary based on varying search criteria
- Daily court list by court and time
- Property received receipt
- Property released receipt
- Booking activity (e.g., intakes, releases, and transfers)

Standard External Data Exchanges:

- Jail management system
- Arrest
- Regional and state warrant and computerized criminal history repositories, following NCIC standards
- Regional, state, and federal information-sharing systems (e.g., RISS, ARJIS, LInX, 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

17.2 PROCESS SUBJECT

The booking process includes collecting all relevant information on the subject and their arrest details, including charges with corresponding state or municipal codes and numbers, 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 reviews the subject's health. Alternatively, health-related notes may need to be attached to the booking record. Medical cautions should be documented, including universal precautions to inform officers and staff of the need for protective measures when handling the individual. This may include exposure to infectious diseases, other health concerns, or situations where the subject was exposed to a taser or mace, as well as any indication of the use of force required to apprehend the individual. A medical clearance may be required before release or transfer to jail.

This information may be obtained from the arrest report within the RMS. If the arrest report is available, a link should be established between the arrest report, the booking record, and the probable cause affidavit, if required by your state. In most states, the affidavit must be presented to a judge or magistrate within a specified timeframe; otherwise, the individual must be released.

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 subject of arrest 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. Ideally, this checklist is configurable given that questions may change over time. Special attention is given to medical and mental health 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 subject's possession will be inventoried and securely stored while the subject is in custody. If the property is not released to the subject upon their release, it must be handled in accordance with department procedures for property and evidence management. This includes entering the property into the property-evidence section of the records management system and documenting the chain of custody.

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 accommodation is unavailable or the subject's assessment warrants the assignment, such as when medical needs exist or intoxication is a factor.

17.3 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, 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 cases, a visual comparison will be necessary to make a determination.

Fingerprints may be sent to a regional or state Automated Fingerprint Identification System (AFIS) and the FBI Integrated Automated Fingerprint Identification System (IAFIS).

The system should check the Master Name Index plus state, regional, and federal databases for 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 received.

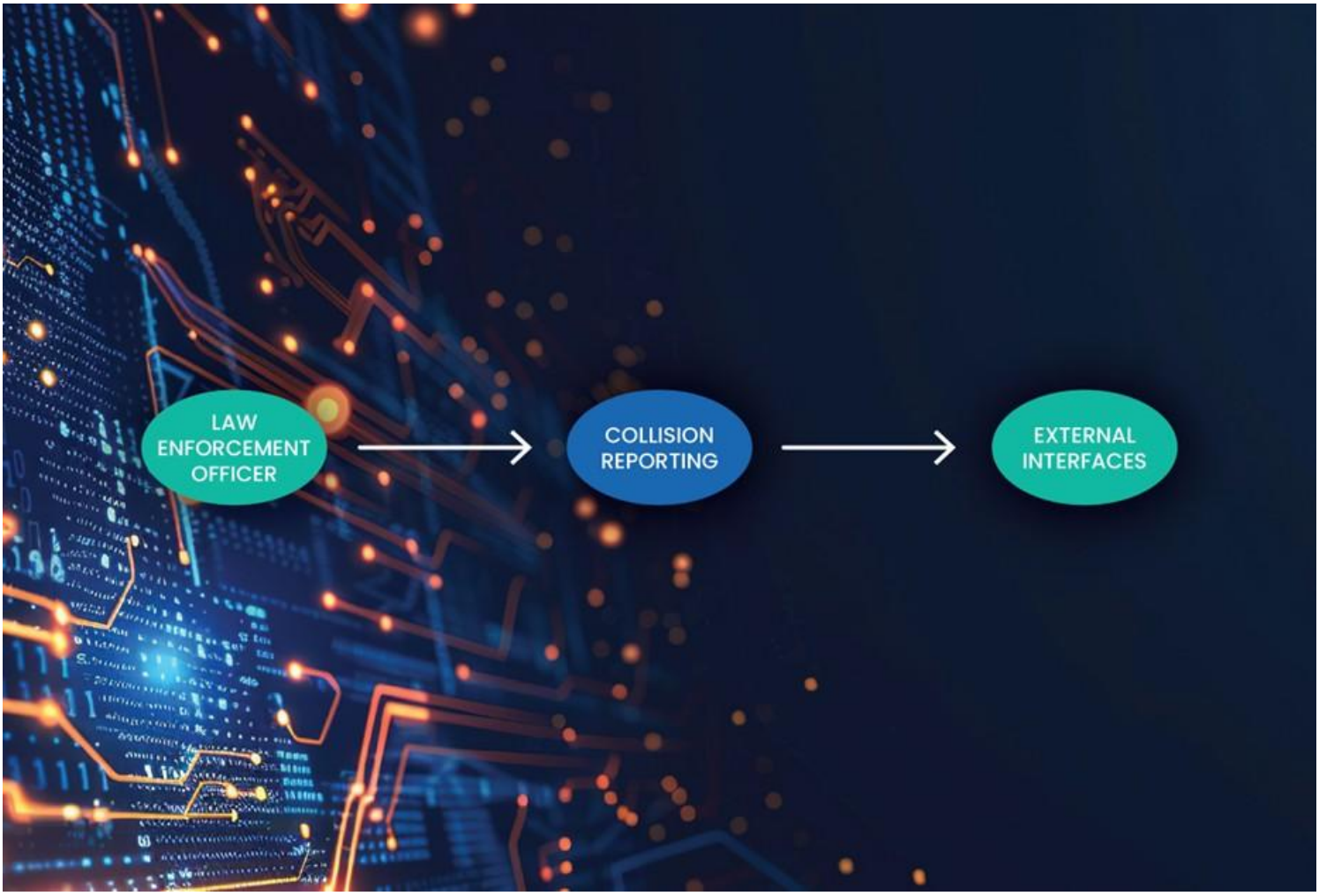
17.4 RELEASE

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. Before release, subjects may have their personal property returned to them. Where applicable, the booking record will be updated to record all relevant information supporting the subject's release 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.*

CHAPTER 18 | COLLISION INVESTIGATION/REPORTING

18.1 COLLISION INVESTIGATION/REPORTING DIAGRAM



Collision investigations and reporting involve the documentation of facts surrounding a traffic crash. Typically, these incidents involve one or more motor vehicles but may also include pedestrians, cyclists, animals, or other objects. Collision reporting may also be referred to by the terms "Crash" or "Traffic Accident." Collision reporting is dictated by the Model Minimum Uniform Crash Criteria (MMUCC) reporting standards provided by the National Highway Traffic Safety Administration. However, many states alter the standard to meet their specific needs. Each state typically has a standard collision report form that must be used for all traffic accidents.

Most states require law enforcement to provide uniform documentation and reporting on all collisions. The information compiled in collision reports is used by the public, insurance companies, traffic analysts, and prosecutors.

Collision reporting may assist in identifying necessary road improvements and eliminating traffic safety hazards. Typically, collision reporting is a module within the agency RMS. The information is 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 or public safety department. If a traffic collision results in the issuance of a citation or criminal report, the appropriate data should transfer between modules to reduce duplicate data entry.

In some jurisdictions, collision reporting is performed using a separate software system, which the state or third-party service provider may provide. It is important to understand state requirements for reporting collision data. Sometimes, the agency may use the state systems and require an interface to the RMS to store a copy of the report captured in

the state system. When the interface is with the state system, updates should occur when made to either the local RMS or the state system. Regardless of where the data is entered, the local agency owns it and is responsible for ensuring accuracy. Consideration should also be given to sharing this data with regional, state, and federal information-sharing systems.

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

Standard Outputs:

- State crash report
- Collisions by location
- Collisions by time of day and day of week
- Collisions by violation
- Collisions by severity
- Collisions by severity of injury
- Collisions by driver demographic
- Collisions by vehicle type
- Driver at fault
- Pedestrian involvement
- Citation(s) issued
- Statistical summary by intersection
- Statistics by area (e.g., address and cross-street locations, beat, precinct, etc.)

Standard External Data Exchanges:

- State motor vehicle division
- Local, regional, and state transportation departments, using National Traffic Safety Highway Administration Standards
- Citation module
- Master Name Index
- Master Vehicle Index
- Mater Property Index
- Arrest Module
- Booking Module
- Property and Evidence Management module
- Fleet Management module

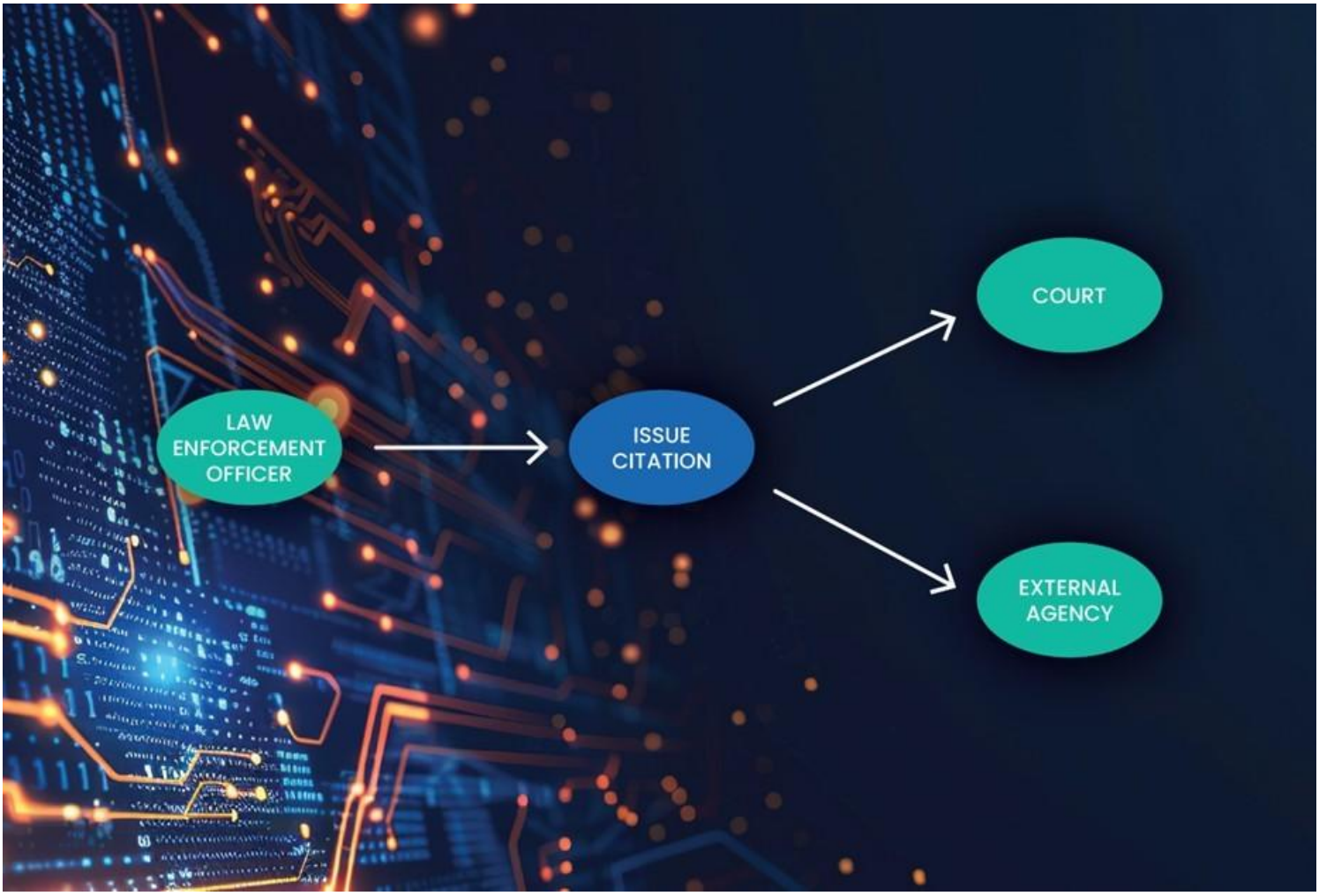
18.2 COLLISION REPORTING

Collision reporting requirements differ from general criminal incident reports in that they emphasize the cause of the crash, including 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 capture crash scenes and location information accurately. These are typically third-party tools. Law enforcement agencies should ensure the costs are factored into their contracts.

The system should allow users to attach diagrams, photographs, and other pertinent documents to the crash investigation. If a citation is issued, or an incident report is taken, as a result of the crash, it 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 subject to multiple levels of approval, and the workflow should be automated.

CHAPTER 19 | CITATIONS

19.1 CITATIONS DIAGRAM



Individuals or organizations charged with minor offenses are often 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 user should also have the ability to issue a warning instead of a citation. 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. Agencies should also be aware of NIBRS reportable misdemeanor offenses when using citation modules. While agency policy may be to issue a citation, completion of an incident report may be required for NIBRS reporting.

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 by receiving a paper or an electronic copy of the citation data. Often, the offender can pay a fine or forfeit a bail amount to satisfy the fine. If the court date is not assigned when the citation is issued, it is assigned later. 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 the officer. The officer must have the ability to print, text a link to, and/or email the citation at roadside.

Many states require all law enforcement agencies to use a uniform citation form and provide an accounting for all citation numbers issued to the officer. The software that

supports the creation of the citation may be a module of the RMS or a third-party solution designed to create 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 the entry of the citation at a later date. The citation module should track all voided citations and warnings issued to the offender. If the stop requires a criminal report, shared information should be transferred between the modules as appropriate. It is important to ensure that data fields are consistent across modules to allow for the seamless transfer of information from one module to another.

Standard Outputs:

- Printed copy of e-citation
- Citation and warnings summary based on varying search criteria
- Citation by location
- Citation by type (traffic, misdemeanor)
- Citation by offense/charge
- Citation by vehicle type
- Citation by address, intersection, mile marker
- Citation by driver license type (commercial, motorcycle license)
- 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, 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

19.2 ISSUE CITATION

Citation information is stored and tracked in the RMS. Officers will document information about the violation(s) or charge(s) and relevant court information. The citation information is then sent to the court, either electronically, if the appropriate interface is in place, or manually. Citation types may include traffic citations, local ordinances, or other types of civil citations or warnings.

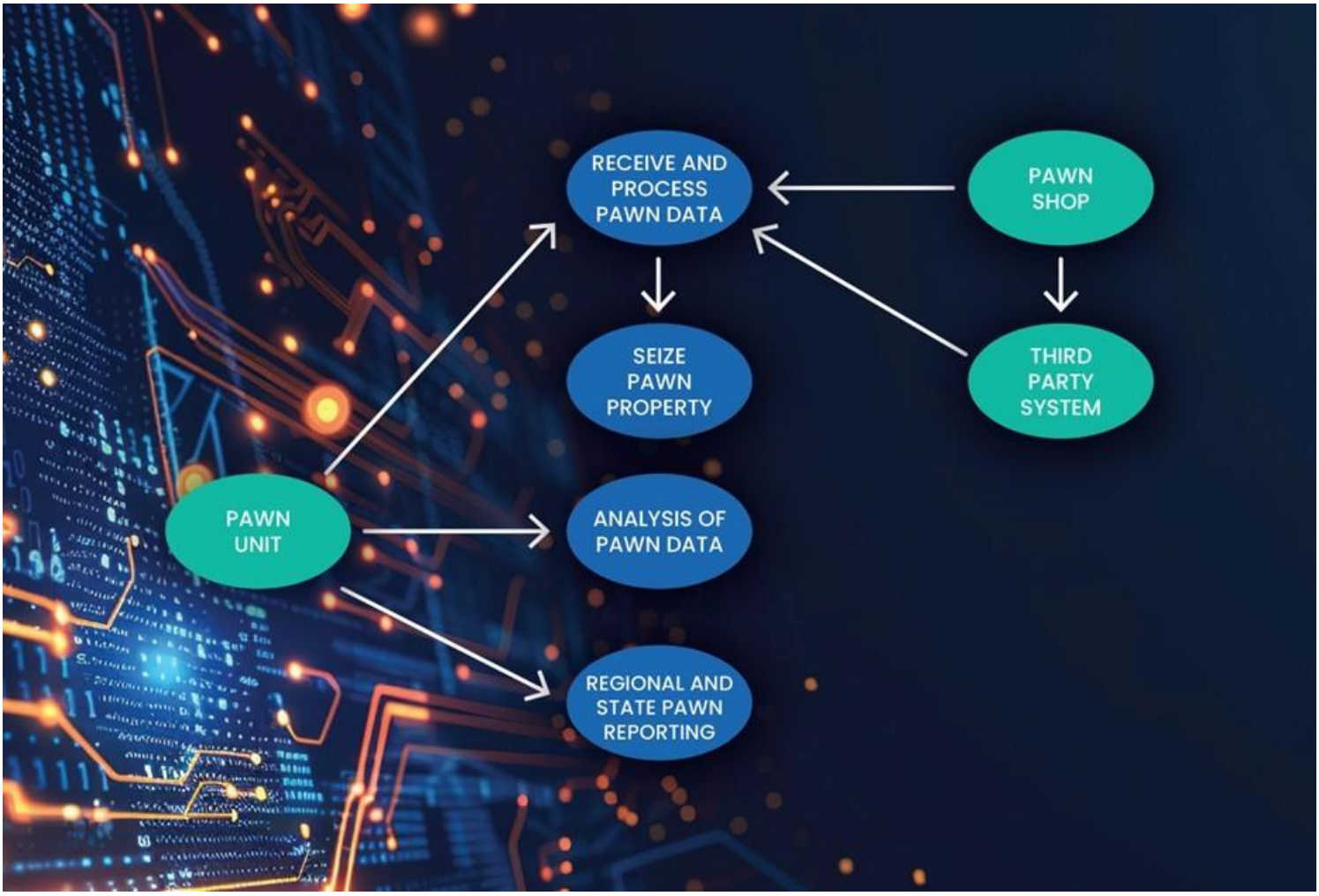
The officer issuing the citation needs to query state and local databases that contain information regarding previously issued citations and warnings. The query should also check for any outstanding warrants or alerts.

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 should also allow the law enforcement officer to collect data on the demographics of the people involved for statistical reporting.

CHAPTER 20 | PAWN

20.1 PAWN DIAGRAM



Pawn modules in RMS help law enforcement representatives identify and recover personal or commercial property that has been reported stolen. Collecting and reconciling pawn information is essential, whether within the RMS or through a third-party system that can be interfaced with the RMS. Many jurisdictions require pawn shops, secondhand dealers, and scrap metal purchasers 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.

The Pawn module should collect, store, and track pawn data. The information received from pawn shops is compared with reported loss and stolen property information. The pawn data also supports the investigative process by allowing for the review of patterns of property sold to pawn shops. The pawn module should also serve the needs of the state pawn systems through interfaces and running inquiries to external regional, state, and federal 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

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, OHLEG)

Standard Internal Data Exchanges:

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

20.2 RECEIVE AND PROCESS PAWN DATA

The pawn shop must submit pawn tickets electronically or on paper to the law enforcement agency. This information is then entered into the Pawn module. If using a third-party product to collect point-of-sale information on behalf of the law enforcement agency, ensure that the system can export data for inclusion in the RMS. The data collected in the RMS should conform with state or local laws pertaining to retention times of property transaction records and be able to produce a purge schedule or purge automatically.

If 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. Name inquiries may be made to state and national systems depending on the type of property being pawned.

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 pawned. Any positive hits that return from these external inquiries require follow-up from the pawn unit or officer assigned this responsibility. This follow-up could include seizing property or further investigation.

20.3 SEIZE PAWN PROPERTY

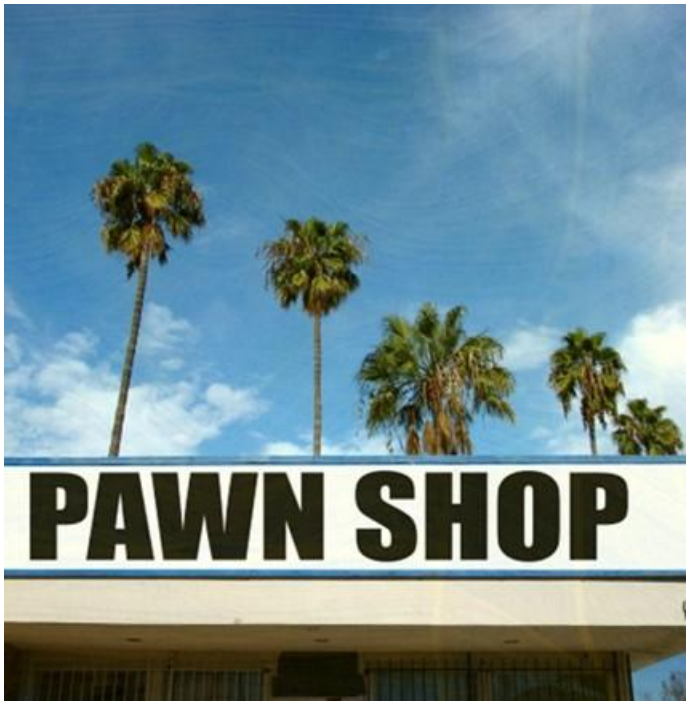
When the pawn unit has identified pawned property that was reported stolen, the pawn record is updated to reflect that the article had been reported stolen and then seized. The pawn unit will take action to seize the property for evidentiary or safekeeping purposes. The property is then checked into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

20.4 ANALYSIS OF PAWN DATA

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

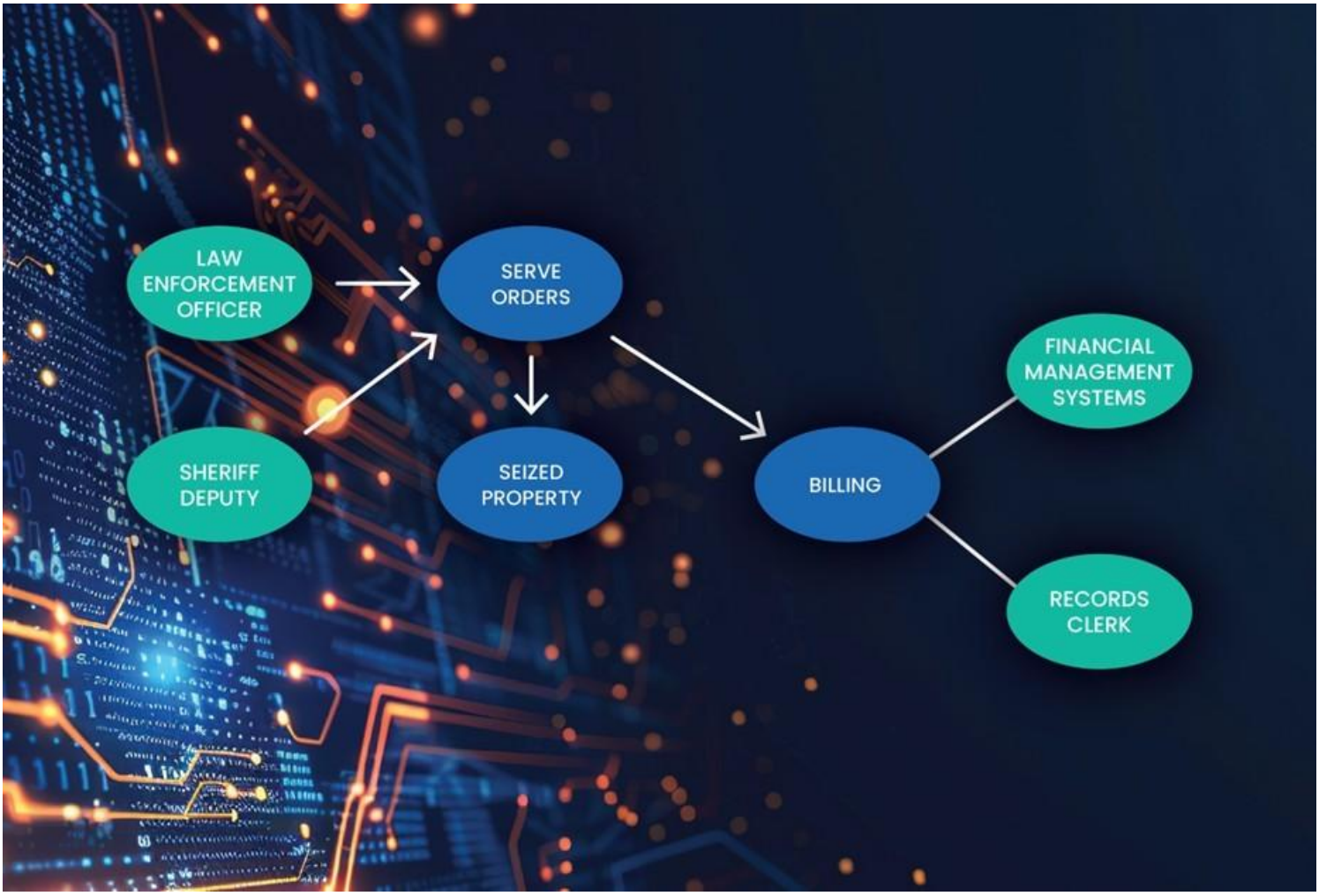
20.5 REGIONAL AND STATE PAWN REPORTING

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



CHAPTER 21 | CIVIL PROCESS

21.1 CIVIL PROCESS DIAGRAM



Civil process describes the law enforcement agency's responsibility to serve legal papers and execute legal processes as required to facilitate due process through the judicial system. The county sheriff commonly performs these functions 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 allow the recording of the disposition of all actions required by the order, including court-ordered eviction, property seizure, and collection of court-ordered fees.

Standard Outputs:

- Active civil papers (e.g., by age, jurisdiction, and server)
- Served/returned civil papers
- Civil paper/civil paper jacket
- Expired civil papers
- Notice generation
- Letter generation
- General financial
- Civil summary (e.g., paper summary, assignments, and attempts to serve)
- Affidavit of service

Standard External Data Exchanges:

- Accounting system
- Court
- Jail management system

Standard Internal Data Exchanges:

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

21.2 SERVE ORDERS

Orders to individuals or organizations are served based on court orders or subpoenas. Service of orders also includes evictions. The law enforcement agency will make a good faith effort to serve the order as often 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.

21.3 SEIZED PROPERTY

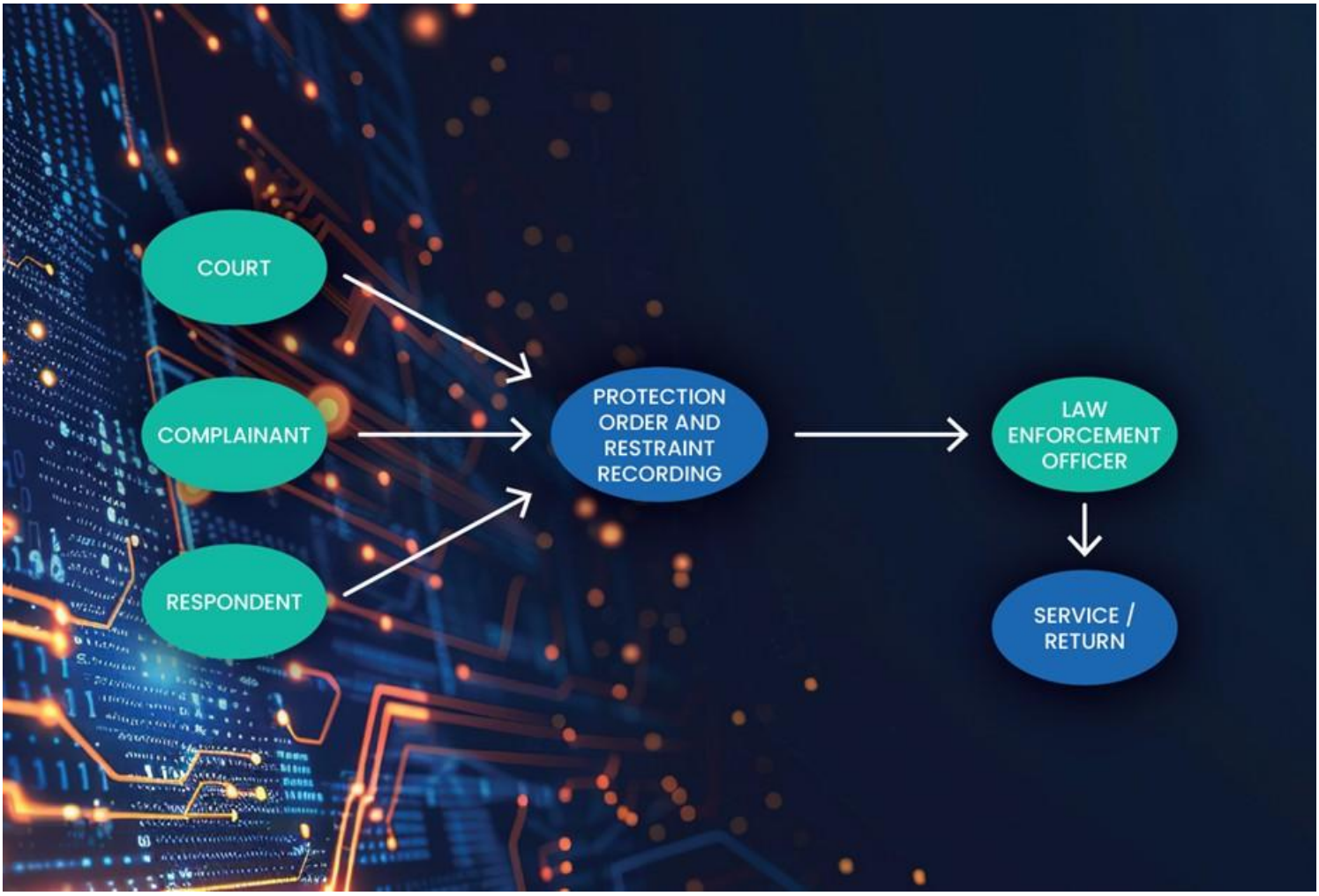
Seized property describes the process and action of seizing personal property based on a court order presented to a law enforcement officer. The individual or organization is served the order to voluntarily relinquish the property. On failure to relinquish property on a designated date, a property seizure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

21.4 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.

CHAPTER 22 | PROTECTION ORDERS AND RESTRAINTS

22.1 PROTECTION ORDERS AND RESTRAINTS DIAGRAM



Law enforcement agencies receive court orders for protection directly from the court or the protected party. This module records protection orders and restraints, including anti-harassment 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 also stored. The conditions should include information such as the issuing authority, effective time period, location, distance, restrictions, and type of prohibited contact. This information must be readily available by name and location of the parties, and may also be cross-referenced by vehicle. Many states have a state-level Protection Order Registry. If possible, the RMS should interface with this system. Many agencies may utilize only the state Protection Order Registry and choose not to capture this information in their RMS. If the data is captured in the RMS, it is essential to remember that updates to the RMS should also be made in the state and NCIC systems. Ideally, the state will allow an interface for the seamless transfer of data.

Standard Outputs:

- Expired/soon-to-expire orders
- Active orders
- Orders that have been served
- Orders received, by source
- Cancelled orders
- No trespass orders
- Service history

Standard External Data Exchanges:

- CAD
- Court

- State, regional, and NCIC Protection Order File management system

Standard Internal Data Exchanges:

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

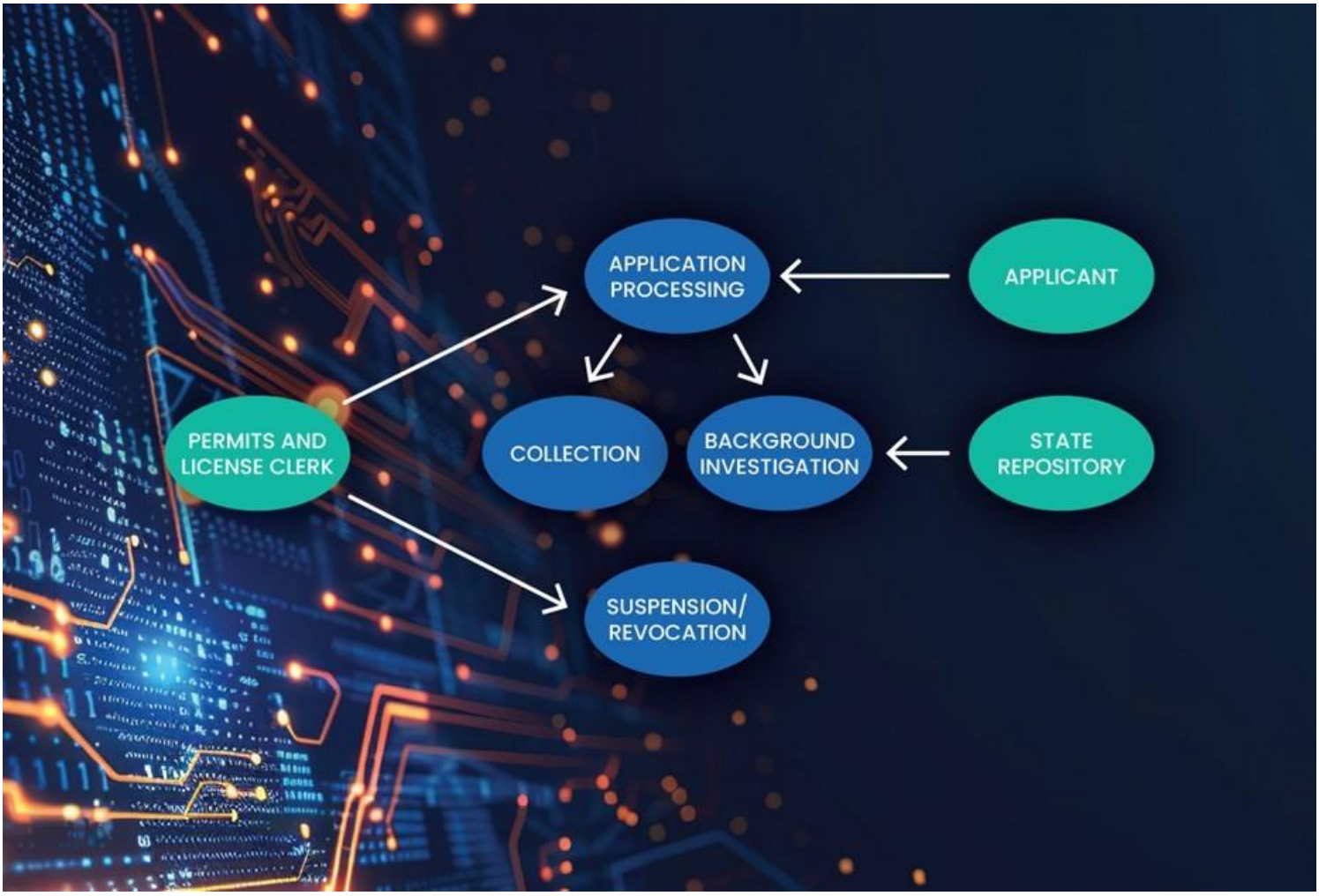
22.2 PROTECTION ORDER AND RESTRAINT RECORDING

The NCIC 2000 Protection Order File is a national registry that allows courts to add, update, and clear orders of protection that a civil or criminal court has issued. As of the end of 2024, 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's 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 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 23 | PERMITS AND LICENSES

23.1 PERMITS AND LICENSES DIAGRAM



The Permits and Licenses module records and tracks the issuance of permits and licenses. 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, while permits provide authority for a shorter and more specific period.

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 or permit.

Once a license or permit is issued, if the licensee is arrested or is issued a traffic violation, the system will generate an alert and notify the permit and license group to determine whether the license should be revoked. The system also must track the payments associated with the issuance of licenses and permits or link with a financial system to determine payment status.

Standard Outputs:

- Permit and license applications granted based on varying search criteria
- Permit and license applications denied with reason
- False alarm responses (for billing purposes)
- Expiration notices
- Renewal Notices

- Violation 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

23.2 APPLICATION PROCESSING

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

Guidelines for approval may include successful completion of required training and/or passing a background check to verify the absence of relevant criminal history information. The application process may involve fees and inspections depending on the license type.

23.3 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.

23.4 BACKGROUND INVESTIGATION

The background investigation aims 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 to obtain a permit. The RMS may include the capability to conduct the background check via the RMS directly in those states where a fingerprint-based check is not required.

23.5 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. A license may also be terminated if the licensee does not adhere to renewal requirements. The above situation can result in the generation of a notification letter to the licensee.

CHAPTER 24 | EQUIPMENT AND ASSET MANAGEMENT

24.1 EQUIPMENT AND ASSET MANAGEMENT DIAGRAM

Law enforcement equipment and assets refer to items owned or leased by the department necessary for the agency's 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., if the equipment is not tracked and maintained properly, it may ultimately impact officer and public safety.

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
- Track disposal of surplus or decommissioned equipment

The integration of barcoding equipment, RFID, etc., may facilitate equipment management and tracking. The system should be able to store photographs of the equipment. The Equipment and Asset Management module should generate reports to support physical inventory and audits, which will assist in managing the repair, disposal, and maintenance of agency equipment.

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

Standard Outputs:

- Physical inventory report based on varying search criteria (e.g., category, age, 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

24.2 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.

24.3 EQUIPMENT ISSUANCE

Equipment may be assigned to an agency unit, division, or group, a physical location, or an individual. In addition, equipment may be allocated 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.

24.4 EQUIPMENT CHECKOUT

When equipment is checked out to a unit or authorized person, information about the checkout (e.g., the individual receiving equipment, the date and time of equipment checkout, and the equipment condition are recorded for tracking purposes. The use of barcode or RFID equipment may facilitate this process.

24.5 EQUIPMENT CHECK-IN

The return of equipment will include an evaluation of the item's condition, 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.

24.6 PHYSICAL INVENTORY/AUDIT

Physical inventory audits require that the RMS generate reports about the physical whereabouts of agency equipment. A physical inventory will identify missing equipment and equipment recommended for repair, replacement, or disposal. This process may determine that the equipment's location has changed. All information gathered during the physical inventory is used to update the system.

24.7 EQUIPMENT MAINTENANCE

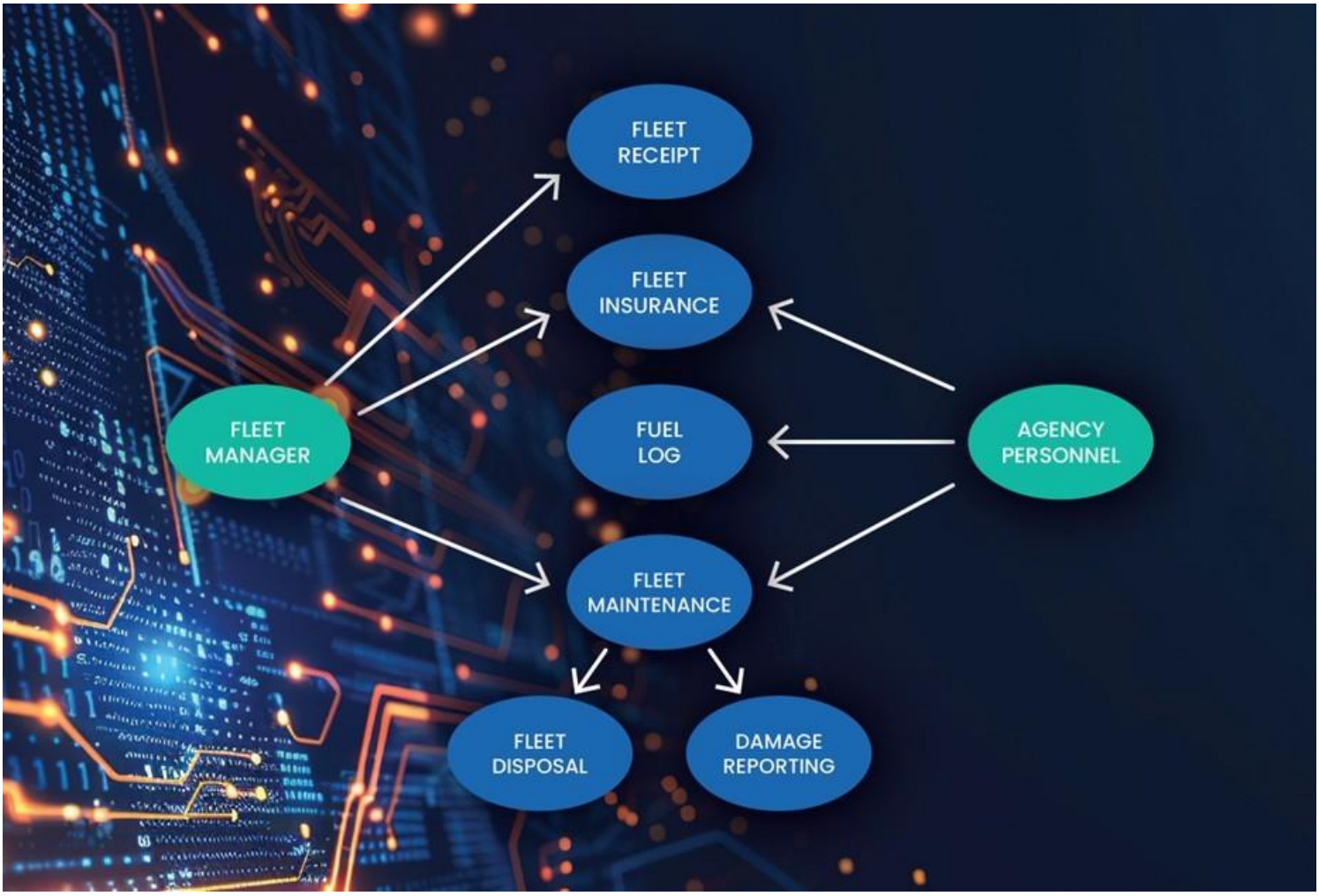
The system should record information about equipment condition and maintenance. The information recorded in this module includes the reason for repair, cost of repair, date of repair, maintenance location, date expected back in service, date returned to service, and date of next scheduled maintenance.

24.8 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 25 | FLEET MANAGEMENT

25.1 FLEET MANAGEMENT DIAGRAM



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

- Integrated with the vehicle's onboard 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 vehicles and related damage/accidents)

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

25.3 FLEET ISSUANCE

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

25.4 FUEL LOG

The Fleet Management module records the date, price, and amount of fuel purchased at each fill-up, the vehicle's mileage at the time of fill-up, and the person completing the 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.

25.5 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 service
- Service provider 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 need unexpected repair.

25.6 DAMAGE/COLLISION REPORTING

Agency personnel and the fleet manager will periodically assess the vehicle's condition and record any damage. Collisions involving fleet vehicles should capture the collision factors and the 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.

25.7 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 26 | PERSONNEL

26.1 PERSONNEL DIAGRAM

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 citizens' academy). This information typically consists of 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 is also 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 functions unique to a law enforcement agency and/or that are typically not found in a stand-alone human resources software program.

The Health Insurance Portability and Privacy Act (HIPAA) regulations apply to agencies that provide health care. To determine whether your system falls under the purview of HIPAA, refer to their website in the resources section.

Standard Outputs:

- Personnel summary, based on varying search criteria
- Personnel detail
- Duty roster
- Training and certification scheduling
- Pending certification and skill expiration
- Issued equipment based on varying search criteria
- Health maintenance requirements for duty status
- Paid detail or detail scheduling

Standard External Data Exchanges:

- Human resources system
- Staffing deployment system (scheduling and assignment)
- CAD

Standard Internal Data Exchanges:

- Equipment and Asset Management module
- Fleet Management module

26.2 PERSONNEL INFORMATION

The system must allow for the gathering and maintenance of basic information for all department personnel or be updated through an API with a separate human resource system. Information may include names, 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 background check information. This information should include when the background check was completed, what sources were used for the background check, and renewal dates for rechecking information sources.

Health maintenance is essential to agency productivity, and some aspects of protecting employee health are mandated by law. The Personnel module will support tracking required vaccinations and medical baselines, such as titer tests for tuberculosis exposure or lead exposure levels of individuals working in firearms training. 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 the 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.

26.3 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 and may generate automatic notifications to staff.

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

26.4 EMPLOYEE PERFORMANCE, SCHEDULING, EXCEPTIONS, AND ADDITIONAL FUNCTIONS

Some RMS products may offer features for tracking employee performance evaluations, including monitoring due dates and performance across categories, as well as documenting training and responses. Additionally, scheduling functionality may allow for the creation of shift patterns and assigning personnel to shifts, locations, and duties. The system may also document schedule exceptions, such as training, leave, or other duties outside the assigned pattern. While potentially useful, these features are generally considered supplementary and not core to the RMS offering.

Some RMS systems include overtime and secondary employment tracking, with workflows for assignment approval, details about the employment (e.g., business name, hours worked), and expiration/renewal dates. Alerts can notify when such assignments conflict with regular duty schedules, although this functionality is not essential to the RMS core.

Additionally, some systems may track commendations and awards, including recognition from citizens or supervisors, along with dates and submission details. An early intervention program may also be included, identifying employees needing assistance due to performance or personal issues. This system can use configurable factors to determine need and may require secure integration with other internal systems, such as internal affairs.

In some cases, RMS systems may interface with external manpower deployment systems to update personnel records and generate duty rosters based on schedules, assignments, and exceptions. While these features can support personnel management, they are not central to an RMS system's core functionality.

CHAPTER 27 | INTERNAL AFFAIRS

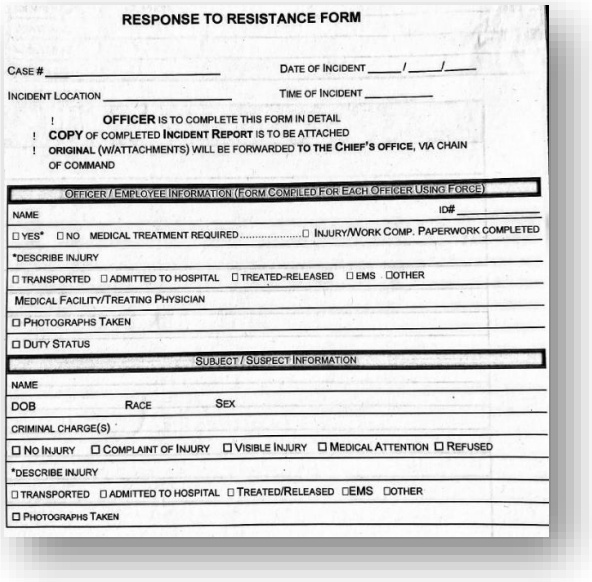
27.1 INTERNAL AFFAIRS DIAGRAM

A law enforcement agency's internal affairs (IA) Division investigates department personnel for incidents and possible suspicions of violations of law and professional misconduct. Several common administrative requirements 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 individual or groups of fields. The system should be permission-based, only permitting those who need access to the information with the proper rights to 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 be able to conduct analysis and 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. 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. IA investigations are often conducted similarly 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.



RESPONSE TO RESISTANCE FORM

CASE # _____ DATE OF INCIDENT ____/____/____

INCIDENT LOCATION _____ TIME OF INCIDENT _____

! **OFFICER** IS TO COMPLETE THIS FORM IN DETAIL
! **COPY** OF COMPLETED **INCIDENT REPORT** IS TO BE ATTACHED
! **ORIGINAL** (W/ATTACHMENTS) WILL BE FORWARDED **TO THE CHIEF'S OFFICE**, VIA CHAIN OF COMMAND

OFFICER / EMPLOYEE INFORMATION (FORM COMPILED FOR EACH OFFICER USING FORCE)

NAME ID# _____

☐ YES* ☐ NO MEDICAL TREATMENT REQUIRED..... ☐ INJURY/WORK COMP. PAPERWORK COMPLETED

*DESCRIBE INJURY

☐ TRANSPORTED ☐ ADMITTED TO HOSPITAL ☐ TREATED-RELEASED ☐ EMS ☐ OTHER

MEDICAL FACILITY/TREATING PHYSICIAN

☐ PHOTOGRAPHS TAKEN

☐ DUTY STATUS

SUBJECT / SUSPECT INFORMATION

NAME

DOB RACE SEX

CRIMINAL CHARGE(S)

☐ NO INJURY ☐ COMPLAINT OF INJURY ☐ VISIBLE INJURY ☐ MEDICAL ATTENTION ☐ REFUSED

*DESCRIBE INJURY

☐ TRANSPORTED ☐ ADMITTED TO HOSPITAL ☐ TREATED/RELEASED ☐ EMS ☐ OTHER

☐ PHOTOGRAPHS TAKEN

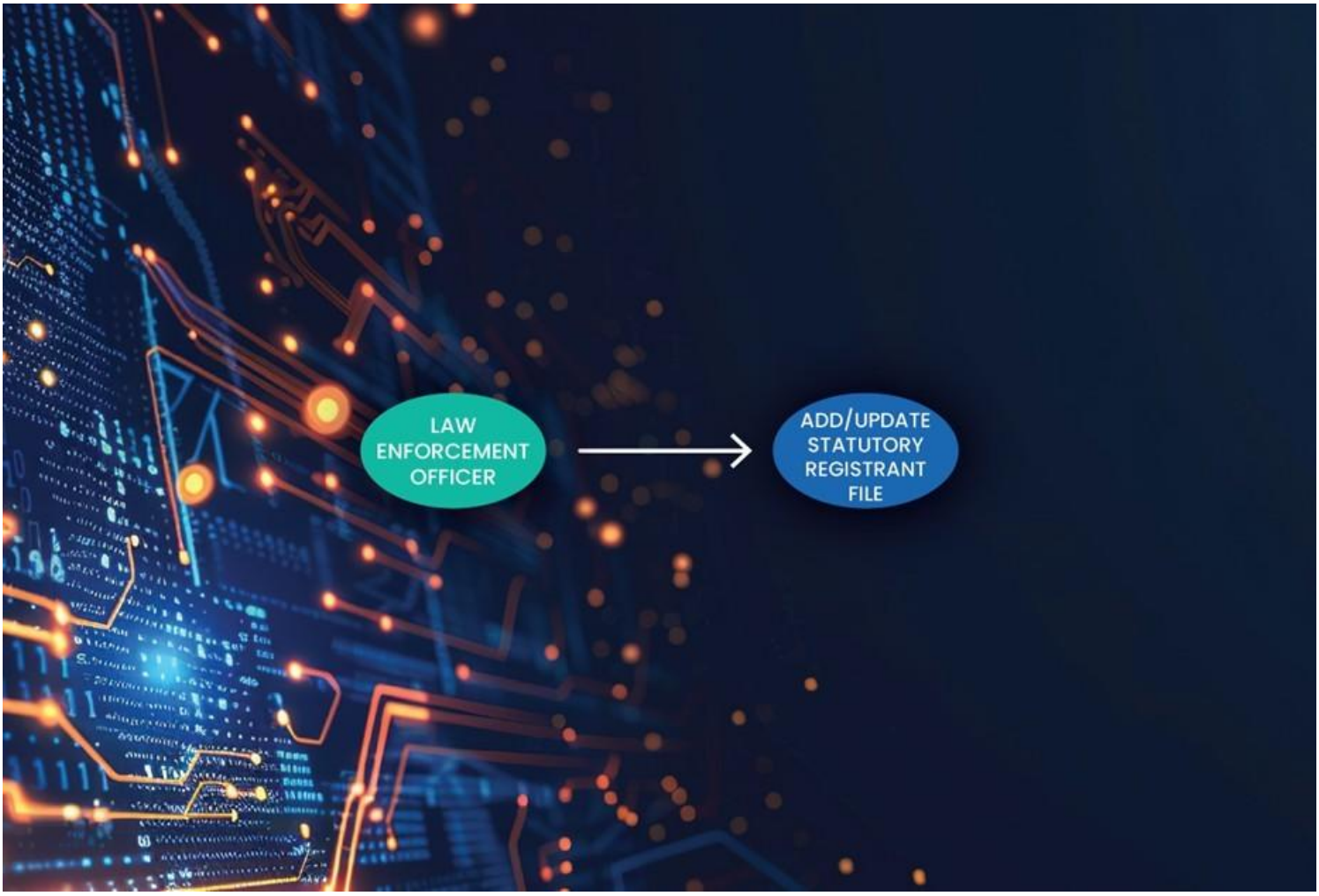
27.2 REPORTING

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 28 | REGISTRATIONS

28.1 REGISTRATIONS DIAGRAM



Local, state, tribal, and federal governments are increasingly enacting statutes that require the registration of individuals convicted or charged with specific offenses. These offenses often include sex crimes, violent offenses, gang membership, arson, compulsive gambling, and other behaviors subject to mandatory reporting and ongoing oversight. These legislative mandates place growing operational and compliance responsibilities on law enforcement agencies, which are typically required to manage, maintain, and monitor these registries to ensure public safety and legal compliance.

Registrations may be maintained in stand-alone systems, separate from the agency's RMS. To support operational efficiency and minimize redundant data entry, the RMS should include the capability to query the registration system using relevant criteria such as name, address, or associated property. The RMS should also support the ability to export relevant data to external registration systems as required by jurisdictional policy, ensuring data consistency and compliance with statutory requirements.

For entry purposes, the RMS should support the ability to add, update, and manage any mandatory registration within the system, with configurable fields to accommodate a wide variety of offense types, statutory requirements, and agency-specific policies. Registries must adhere to all applicable local, state, and federal laws governing registration requirements, the publication and mapping of registrant information, personal privacy protections, and public records regulations.

Registrations must be kept current and updated regularly in accordance with required reporting intervals. The RMS should be able to generate automated alerts to designated personnel if a registrant fails to comply with mandated re-registration timelines. In addition, the system should automatically cross-reference the registrant's current residence with a list of restricted zones, such as schools,

daycare facilities, and other protected areas, and issue warnings or notifications when a violation or proximity risk is detected.

By supporting comprehensive registration management and integrating with external systems, the RMS can play a vital role in ensuring accurate oversight of registrants, maintaining public trust, and enabling agencies to meet both their legal and operational obligations.

Standard Outputs:

- State, regional, and federal information-sharing systems (e.g., RISS, ARJIS, LInX, N-DEx, ISE)
- Registration status reports (compliant, non-compliant, overdue)
- Historical registration activity and changes
- Automated notifications for upcoming or missed registration deadlines
- Residency verification reports and alerts
- Audit logs of updates and user interactions with registration records
- Statistical summaries by offense type, location, compliance status, and demographics
- Maps showing proximity of registrants to restricted zones (based on agency policy)

Standard External Data Exchanges:

The RMS should support data exchange with external state, regional, and federal systems to ensure compliance, support investigations, and promote interoperability. Examples include:

- State and federal sex offender registries
- National Data Exchange (N-DEx)
- Law Enforcement Information Exchange (LInX)
- Regional Information Sharing Systems (RISS)
- Automated Regional Justice Information System (ARJIS)
- Information Sharing Environment (ISE)
- State-level criminal history repositories or corrections databases

Standard Internal Data Exchanges:

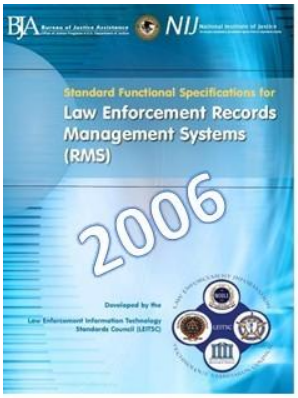
The RMS should be able to share registration-related information internally across modules to streamline operations and ensure consistency. This may include:

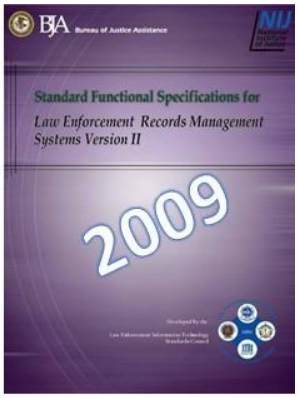
- Case Management Module – linking registration status to investigations or arrests
- Incident Report Module – flagging individuals with active registration status during report creation
- Field Interview or Contact Module – automatically referencing known registrants during officer interactions
- Property and Evidence Module – associating registration status with seized items if applicable
- Notification/Alert Module – enabling supervisory or investigative alerts for compliance issues
- Mapping Module – displaying restricted zones and registrant locations
- Patrol Briefings/Officer Safety Bulletins – integrating registration details into roll call or officer awareness tools

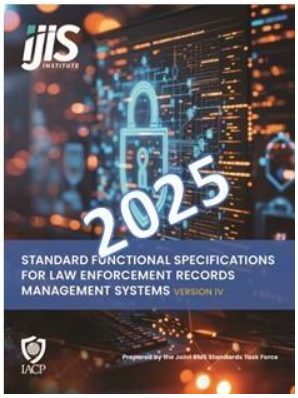
CHAPTER 29 | CONCLUSION

The functional specification document provides a general understanding of what should be included in a modern law enforcement Records Management System (RMS). It serves as a valuable reference for developing agency policies, drafting Requests for Proposals (RFPs), and guiding training development and delivery. Individuals who are new to law enforcement records management will find this an especially helpful resource.

Historically, the lifespan of an RMS ranged from 10 to 20 years. However, due to rapid technological advancement and shifting agency needs, many law enforcement agencies are now replacing systems more frequently. RMS solutions must continuously evolve alongside technology and policy changes. As such, it is important that agencies select providers capable of adapting to the fast pace of innovation offering clear, customer-driven roadmaps.







Given the complexity of RMS implementation, including requirements definition, procurement, data migration, and training, careful planning is critical. As the demands placed on officers and law enforcement agencies continue to increase, it is essential that agencies be supported by up-to-date, efficient, and interoperable technology, reducing duplicative effort and enhancing productivity.

When considering a new RMS or upgrading an existing one, agencies must understand how local, state, and national laws and policies influence system requirements and procurement. It is equally critical to recognize that crime does not stop at jurisdictional boundaries. While the importance of information sharing has been widely discussed for decades, significant work remains. Achieving seamless interoperability depends on the implementation of modern solutions based on open standards that facilitate secure, effective sharing with neighboring agencies and with state, national, and international systems.

Security and privacy are of the utmost importance. Over the past several years, law enforcement has made significant progress in areas such as cyber defense and compliance with the FBI's Criminal Justice Information Services (CJIS) Security Policy. At the same time, the public's expectation for transparency continues to grow. Agencies must ensure that RMS data can be used for timely reporting and analysis while maintaining appropriate safeguards for sensitive information.

Striking a balance between security, privacy, and transparency is challenging but achievable. An effective RMS should empower agencies to access, analyze, and report data quickly while ensuring that all activities are compliant with applicable policies and regulations.

This document should be considered a baseline from which agencies can develop software requirements to include in an RFP. Successful procurements are typically the result of well-documented, clearly defined requirements that align with agency operations and future goals. The functional areas outlined in this publication reflect both core and optional capabilities to support sound recordkeeping, operational efficiency, and transparency.

Finally, when using this document, agencies are encouraged to consider the broader trajectory of technological advancement. RMS platforms must be designed to work smarter and more efficiently. In the years ahead, capabilities such as report completion through voice recognition, mobile-friendly RMS applications accessible on any device, and the use of configurable, database-driven forms are expected to become standard. Most importantly, the law enforcement community must continue to promote the adoption of open standards to support data interoperability and information sharing. Doing so will help achieve the ultimate goal: understanding, preventing, and reducing crime.

APPENDIX A | LIST OF ACRONYMS

ABAC	Attribute-Based Access Control
AFIS	Automated Fingerprint Identification System
AI	Artificial Intelligence
API	Application Programming Interface
ARJIS	Automated Regional Justice Information System
BJA	Bureau of Justice Assistance
BJS	Bureau of Justice Statistics
BWC	Body Worn Camera
CAD	Computer-Aided Dispatch system
CALEA	Commission on Accreditation for Law Enforcement Agencies
CFS	Calls for Service
CHRI	Criminal History Record Information
CIT	Crises Intervention Team
CJIS	Criminal Justice Information System
CMS	Case Management System
COTS	Commercial Off the Shelf
CSO	CJIS Security Officer
DMV	Department of Motor Vehicles
DNA	Deoxyribonucleic Acid
DOJ	United States Department of Justice
DPA	Data Protection Act (UK)
DPPA	Driver's Protection and Privacy Act
DUI	Driving Under the Influence
EFTS	Electronic Fingerprint Transmission Specification
FBI	Federal Bureau of Investigation
FIPS	The Federal Information Processing Standards
GDPR	General Data Protection Regulation (UK)
GIS	Geographical Information System
HIPAA	Health Insurance Privacy and Portability Act
IA	Internal Affairs
IACA	International Association of Crime Analysts
IACP	International Association of Chiefs of Police
IAFIS	Integrated Automated Fingerprint Identification System, an FBI system
IBRS	Incident-Based Reporting System
ICAM	Identity, Credential, and Access Management
IEPD	Information Exchange Package Document
ISE	Information Sharing Environment
IJIS	Integrated Justice Information Systems Institute
JMS	Jail Management System
JRA	Justice Reference Architecture
JSON	JavaScript Object Notation
LEA	Law Enforcement Agency
LEAC	IJIS Law Enforcement Advisory Committee
LEITSC	Law Enforcement Information Technology Standards Council
LInX	Law Enforcement Information Exchange, an NCIS System
MFA	multi-factor authentication
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
N-DEx	National Data Exchange, an FBI System
NCIC	National Crime Information Center
NCIS	Naval Criminal Investigative Service
NIBRS	National Incident-Based Reporting System
NIEMOpen	National Information Exchange Model
NISP	National Industrial Security Programme (UK)
NIST	National Institute of Standards and Technology

Nlets	International Justice and Public Safety Information Sharing Network
NMVTIS	National Motor Vehicle Title Information System
NOBLE	National Organization of Black Law Enforcement Executives
NSA	National Sheriffs' Association
NTSHA	National Traffic Highway Safety Administration
OAN	Owner Applied Number
OASIS	Organization for the Advancement of Structured Information Standards
OAUTH	Open Authorization
ODBC	Open Database Connectivity
OHLEG	Ohio Law Enforcement Gateway
OJP	Office of Justice Programs
ORI	Originating Agency Identifier
OUI	Open Use Initiative
PDF	Portable Document Format
PII	Personally Identifiable Information
REST	Representational State Transfer
RFI	Request for Information
RFID	Radio Frequency Identification
RFP	Request for Proposal
RISS	Regional Information Sharing Systems
RMS	Records Management System
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAR	Suspicious Activity Report
SFTS	Standard Field Sobriety Test
SID	State Identification Number
SOA	Service-Oriented Architecture
SOC 2	Systems and Organizational Controls 2
SOP	Standard Operating Procedure
SRS	Summary Reporting System
SSN	Social Security Number
UCN	Universal Control Number
UCR	Uniform Crime Reporting
VIN	Vehicle Identification Number
XML	Extensible Markup Language

APPENDIX B | GLOSSARY

ACCREDITATION: The formal recognition bestowed upon a police agency or law enforcement organization that meets specific standards established by an authoritative body.

AD HOC REPORTING: Custom analysis and operational reports that are created when not provided by the RMS.

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.

ARTIFICIAL INTELLIGENCE: The simulation of human intelligence in machines that are programmed to think and learn. These systems can perform tasks that typically require human cognitive functions, such as understanding natural language, recognizing patterns, solving problems and making decisions.

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 as an example of regional information sharing.

ARREST: To take someone into custody.

ASSIGNMENT: A portion of the 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.

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

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

BODY WORN CAMERA: A recording device that is attached to a person's body, typically worn on uniform or clothing, to capture audio and video footage of events as they occur.

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 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.

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

CHANGE MANAGEMENT: The systematic approach used to manage the transition and implementation of software systems or updates to existing ones within a law enforcement agency. This process involves planning, coordinating, and evaluating changes to ensure that they are introduced smoothly and with minimal disruption to operations.

COMMISSION ON ACCREDITATION FOR LAW ENFORCEMENT AGENCIES, INC (CALEA): An organization that has established a set of professional standards for law enforcement. Law enforcement agencies can become accredited through the commission once they demonstrate compliance with these standards. Achieving CALEA accreditation signifies that an agency is committed to maintaining high standards of professionalism, accountability, and effectiveness in its operations.

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 bail, and/or appear in court on a specified date. Commonly used in traffic and misdemeanor law enforcement.

CIVIL PROCESS: The law enforcement agency's responsibility to serve legal papers and execute legal process as required to facilitate due process through the judicial system.

COLLISION REPORTING: Module within an RMS. Emphasizes the cause of the crash, weather, visibility, road surface conditions at the time of incident, and location. May also be known as Crash Reporting.

COMPUTER-AIDED DISPATCH (CAD): A computer system that assists 911 operators and dispatch personnel in handling and prioritizing calls.

CONSENT DECREE: A legally binding agreement or order that is entered into between a law enforcement agency and a government entity, often resulting from findings of misconduct or civil rights violations.

CONFIGURABILITY: The ability of the software to be tailored or adjusted to meet the specific needs and requirements of a particular law enforcement agency. This includes enabling users to customize various features, functionalities, and settings without requiring extensive programming or technical skills. Examples include: user roles and permissions, report templates, data fields, workflows, and integrations.

DAMAGE REPORTING: Record of vehicle condition and damage.

DASHCAMS: Dashboard cameras are recording devices mounted in law enforcement vehicles that capture video and audio footage of events occurring in front of the vehicle.

DATA MANAGEMENT: Involves record expungement and sealing, data redaction, and data dictionary.

DATA PROTECTION ACT (DPA): Legislation that governs the handling, processing, and storage of personal data by organizations, including law enforcement organizations. Its primary purpose is to protect the individual's privacy and personal information while establishing guidelines for how data should be managed to ensure security and integrity.

DIGITAL EVIDENCE MANAGEMENT: Systematic process of collecting, preserving, analyzing, and storing digital evidence derived from various electronic devices and platforms. This evidence can include data from computers, smartphones, digital cameras, social media, and other digital sources relevant to criminal investigations.

DISPOSITION: The final outcome of a case or incident after it has been processed by the police or legal system.

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

ENTITY: Consists of one or more identities that agencies deem to be the same individual.

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 prove or disprove 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 organizations outside of the law enforcement agency.

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).

FedRAMP: The Federal Risk and Authorization Management Program provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud service providers that wish to offer their services to government entities.

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 the vehicle was deployed, starting mileage, and identifiers such as the VIN and license plate number as well as any agency-specific unique identifier) and establishes the service schedule.

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

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

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

GEOGRAPHIC INFORMATION SYSTEM (GIS): A system that captures, stores, analyzes, and manages data and its associated attributes that are spatially referenced to the earth.

GLOBAL JUSTICE REFERENCE ARCHITECTURE (JRA): Framework that outlines the standards, structures, and processes necessary for effectively managing and sharing information across different jurisdictions in the context of justice and public safety.

GovRAMP: The Government Risk and Authorization Management Program, is a U.S. government initiative to facilitate the adoption of cloud services in federal agencies.

IDENTITIES: Refers to the individual person records that are created by the police agencies.

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 non-criminal 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 NIEMOpen 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.

INTEROPERABILITY: The ability of different systems, devices, and software applications used by various law enforcement agencies to communicate, exchange, and use information effectively.

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 managed by the Naval Criminal Investigative Service and governed by its member law enforcement agencies. Referenced 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, prosecutors, financial systems, jail management systems, human resources systems, and multi-jurisdictional information systems).

MOBILE DATA COMPUTER: A mobile computer that allows law enforcement officials to interface with department systems while in the field, usually found in law enforcement vehicles.

MASTER LOCATION INDEX (MLI): Provides a means to aggregate information throughout the RMS based on a specific address, a range of addresses, an area (i.e., as defined 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, businesses, schools, 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.

MOBILE TECHNOLOGY: The use of portable devices and applications, such as smartphones, tablets, and laptops, to enhance the efficiency, effectiveness, and responsiveness of police work and public safety operations.

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.

NATIONAL INCIDENT-BASED REPORTING SYSTEM (NIBRS): NIBRS is an incident-based reporting system that collects data on each single incident and arrest within the 28 offense categories that are made up of 71 specific crimes called Group A offenses and arrest data for 10 Group B offenses. (*2023.0 National Incident-Based Reporting System User Manual*).

NATIONAL INFORMATION EXCHANGE MODEL (NIEMOpen): A common vocabulary that can be used by software developers to facilitate communication between information systems.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST): US federal agency within the Department of Commerce that develops standards, guidelines, and best practices for various fields including law enforcement, in the law enforcement context. NIST provides resources related to the management and analysis of digital services, cybersecurity, and biometrics.

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.

OCCURRENCE: A single, distinct event (a call for police services) that may or may not result in criminal offenses. An occurrence refers to one (or more) criminal offense(s) during one single, distinct event.

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

ONLINE CITIZEN REPORTING: The use of a digital platform that allows members of the public to report non-emergency incidents or provide information to law enforcement agencies via the internet.

OPEN DATABASE CONNECTIVITY (ODBC): Provides a standard software application programming interface (API) method for database management systems making them independent of programming languages, databases, and operating systems.

OPENID: Open standard and decentralized protocol that allows users to authenticate with multiple websites using a single set of credentials.

OPERATIONS MANAGEMENT: Organization and management of basic and essential business functions.

ORGANIZATION FOR THE ADVANCEMENT OF STRUCTURED INFORMATION STANDARDS (OASIS) – A non-profit consortium that focuses on the development and adoption of open standards for the global information society. Founded in 1993, OASIS brings together a diverse community of organizations, individuals, and experts to create standards related to various aspects of information interchange, security, and delivery.

ORIGINATING AGENCY IDENTIFIER (ORI): An identifier that 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 more specific period of time.

PERSONNEL: All employed persons within a place of work.

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

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

PROPERTY DISPOSITION: Procedures for the release of property from the system. Property Storage: Movement of property that is recorded to ensure that an accurate log of the activity is captured, and all policies and chain-of-custody rules are followed.

PROTECTION AND RESTRAINING ORDERS: A civil order issued by the court to order a person to cease contact with a person, to stay away, to stop harming, etc.

QUERY: A query occurs when search criteria are transmitted to an external source and search results are returned to the system originating the query. Note that these are not considered exchanges because the 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, prosecutors, 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 collected.

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

REQUEST FOR INFORMATION (RFI): A formal process used by law enforcement agencies to solicit information from service providers about their products, services, and capabilities.

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.

SOFTWARE AS A SERVICE (SaaS): A cloud-based service model that provides software applications over the internet. In this model, applications are hosted on a service provider's infrastructure and made available to users on a subscription basis or through pay-per-use pricing.

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

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

SEIZE PAWN PROPERTY: Taking pawned property that has been identified as stolen into custody for evidentiary or safekeeping purposes.

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

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

STANDARD OPERATING PROCEDURE (SOP): Set of defined standards that are used to perform a given task.

STANDARDIZED REPORTING: A set of standardized reports contained in each 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 stored in state systems (e.g., updates for wanted persons, missing persons, stolen vehicles/property, and state sex offender registries).

STATE PAWN REPORTING: An external repository maintaining pawn data to which local pawn modules may be transmitted electronically.

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

SUBJECT: Person in question.

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

SUSPENSION-REVOCATION: When a license or permit is taken away.

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

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

TRAINING: Instruction and education.

UNIFORM CRIME REPORTING (UCR): The UCR Program is a voluntary city, county, state, tribal, and federal law enforcement program that provides a nationwide view of crime based on the submission of statistics by law enforcement agencies throughout the country.

USE OF FORCE DATA COLLECTION: The FBI data collection program aimed at gathering comprehensive data on incidents involving the use of force by law enforcement agencies.

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 before serving.

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

APPENDIX C | END NOTES

i. NIEMOpen *https://niemopen.org/*

ii. NIST *https://www.nist.gov/*

iii. Global Justice Reference Architecture *https://bja.ojp.gov/program/it/national-initiatives/gra*

iv. Global Privacy and Information Quality Solutions *https://bja.ojp.gov/program/it/global/groups/gpiqs*

v. Fusion Center Guidelines *https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_guidelines_law_enforcement.pdf*

APPENDIX D | 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
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.

Artificial Intelligence Playbook for Justice, Public Safety, and Security Professionals:
https://ijis.org/community-resources/artificial-intelligence-playbook-for-justice-public-safety-and-security-professionals
This playbook developed by the IJIS Institute's Artificial Intelligence Working Group is intended to help users in their journey to develop, implement, or utilize AI-based capabilities, which can be used at any point in the adoption lifecycle.

CJIS Security Policy Resource Center:
https://le.fbi.gov/cjis-division/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://ijis.org/community-resources/cloud-fundamentals
This paper describes the basics of cloud computing and the role that the cloud can play in public safety. It also provides a brief introduction to critical security and compliance considerations.

Defense Counterintelligence and Security Agency (DCSA):
https://www.dcsa.mil
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/app/details/USCODE-2011-title18/USCODE-2011-title18-partI-chap123-sec2721
Prohibition on release and use of certain personal information from State motor vehicle records

Electronic Code of Federal Regulations CFR 28Part 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 that ensures the accuracy, completeness, currency, integrity, and security of such information and to protect individual privacy.

Electronic Code of Federal Regulations CFR 28Part 23:
https://www.ecfr.gov/current/title-28/chapter-I/part-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.

The Federal Information Processing Standards (FIPS):
https://www.nist.gov/federal-information-processing-standards-fips
FIPS are a series of publicly announced standards developed by the National Institute of Standards and Technology (NIST) for use in computer systems by non-military U.S. government agencies and contractors. These standards establish requirements for ensuring computer security and interoperability, particularly in cases where suitable industry standards do not exist.

Fusion Centers and Intelligence Sharing:
https://bja.ojp.gov/program/it/national-initiatives/fusion-centers
Chapter 8 of the Fusion Center Guidelines document specifically speaks to Privacy and Civil Liberties related to data sharing.

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

The IACP Connector:

https://www.theiacp.org/resources/iacp-connector

The law enforcement researcher's friend: Once supported and populated, this curated, current database of law enforcement technology search and procurement successes that connects cops with cops first, and then industry providers for fast and reliable research and deployment results. The IACP Connector is where LE researchers can:

- Come to one place to see relevant, successful tech search, purchase and deployment testimonies
- Connect with cops first, and industry providers when ready
- Conquer technology research challenges

International Association of Chiefs of Police RMS Standards:

https://www.theiacp.org/resources/standard-functional-specifications-for-record-management-systems

The IACP is the world's largest and most influential professional association for police leaders and is a recognized leader in global policing, committed to advancing safer communities through thoughtful, progressive police leadership. IACP partnered with the IJIS Institute to keep the RMS Standards document up to date and available to law enforcement.

International Association of Crime Analysts (IACA):

https://www.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 standards of performance and technique within the profession itself.

IJIS Institute RMS Standards Development:

https://ijis.org/ijis-key-initiatives/rms-standards-development/

The IJIS Institute partnered with the IACP to work on RMS Standards Development. This site includes information on this effort as well as updates.

ISO/IEC 27001:

https://www.iso.org/standard/88435.html

The ISO/IEC 27001:2022 standard, titled "Information security, cybersecurity and privacy protection — Information security management systems — Requirements," is a globally recognized framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). It provides organizations with a systematic approach to managing sensitive information, ensuring its confidentiality, integrity, and availability.

Law Enforcement Information Exchange Program (LInX):

https://www.ncis.navy.mil/About-NCIS/Mission/Partnership-Initiatives/LInX-D-Dex

LInX is a federally funded regional law enforcement information-sharing program sponsored and+ operated by the Naval Criminal Investigative Service. There are 15 LInX Regions in the United States with each Region governing its own regional program. All 15 Regions are connected and have a data exchange partnership with the FBI N-DEx Program allowing users to query both systems together.

National Crime Information Center (NCIC):

https://le.fbi.gov/informational-tools/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.

National Data Exchange (N-DEx) System:

https://le.fbi.gov/informational-tools/national-data-exchange-n-dex

The N-DEx system provides criminal justice agencies with an online tool for sharing, searching, linking, and analyzing information across jurisdictional boundaries. A national repository of criminal justice records submitted by agencies from around the nation, N-DEx enables users to "connect the dots" between data on people, places, and things that may seem unrelated in order to link investigations and investigators.

National Incident-Based Reporting System (NIBRS):

https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/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 Information Exchange Model (NIEMOpen):

https://niemopen.org/

NIEMOpen is a data interoperability framework (formerly known as NIEM) that provides semantic and syntactic standards for data components to enable improved information sharing within and across communities of interest in a variety of domains. Under the auspices of OASIS, the authoritative collaborative that develops standards for data management, NIEMOpen engages federal, state, local, tribal, territorial, and international organizations from the public and private sectors to use standards that enable higher levels of interoperability and less costly exchanges of digital

information to improve mission effectiveness. Newer versions of NIEMOpen support the creation of ontologies for knowledge graph technologies as well as exchanges between and among conventional structured databases. The NIEMOpen framework includes tools and methodologies for the development of information exchange standards and ontologies, all available at no cost.

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 Emergency Number Association (NENA):

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.

NIST 800-53 Security Controls:

https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

The National Institute of Standards and Technology publishes best practice security and privacy controls for information systems and organizations.

NIST Policy Templates:

https://ijis.org/nist-policy-templates-a-resource-for-cjis-security-policy-compliance-and-modernization/

IJIS has highlighted a series of sample policy templates developed by the National Institute of Standards and Technology (NIST). These templates serve as invaluable tools for agencies striving to align with the FBI's Criminal Justice Information Services (CJIS) Security Policy and the FBI's broader modernization initiatives.

Privacy Act of 1974:

https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition

The Privacy Act of 1974 is a pivotal U.S. federal law that governs how federal agencies collect, maintain, use, and disseminate personally identifiable information (PII) about individuals. Enacted in the aftermath of the Watergate scandal, the Act was designed to protect citizens from unwarranted invasions of privacy by establishing a code of fair information practices.

Privacy Impact Assessments:

Resources that might be useful to Law Enforcement Agencies in determining how to conduct a Privacy Impact Assessment.

https://www.dhs.gov/privacy-impact-assessments

The Department of Homeland Security, Privacy Office, includes resources for LEAs to help identify and mitigate privacy risks.

https://www.justice.gov/opcl/doj-privacy-impact-assessments

The Department of Justice, Office of Privacy and Civil Liberties, provides Privacy Impact Assessments Official Guidance.

https://www.govinfo.gov/app/details/PLAW-107publ347

The E-Government Act of 2002, Pub. L. No 107-347, § 208, 116 Stat. 2899, 2921 (2002).

United Kingdom Resources:

Data Protection Act:

https://www.college.police.uk/app/information-management/data-protection

Data protection is a core requirement to support effective policing. It identifies the structures, responsibilities, policies, and processes that must be in place to ensure consistency in the way the DPA and UK GDPR are applied throughout the police service.

General Data Protection Regulation (GDPR):

https://www.gov.uk/guidance/meet-the-requirements-of-data-privacy-regulations

This guide explains the General Data Protection Regulation (GDPR) to help organizations comply with its requirements.

Management of Police Information (MoPI):

https://www.college.police.uk/app/information-management/management-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 risks associated with police information.