

RFQ GG000018,2

Title **Police Records Management System**

Preview Date

Open Date **6/11/2026 12:58 PM**

Close Date **8/5/2026 2:00 PM**

Award Date

Time Zone **Central Standard Time**

Submit your response to the following contact.

Company **Metropolitan Government of Nashville and Davidson County**
Buyer **Terri Lynn Ray**
Location **PO Box 196301**
Nashville, TN 37219
Davidson
United States
Phone **1-615-862-6669**
Fax
E-mail **Terri.Ray@nashville.gov**

When submitting your response, include the following information.

Your Company Name	
Company Site (<i>Optional</i>)	
Address	
Contact Details	
Response Valid Until (<i>Optional</i>)	

This document has important legal consequences. The information contained in this document is proprietary of Metropolitan Government of Nashville and Davidson County. It shall not be used, reproduced, or disclosed to others without the express and written consent of Metropolitan Government of Nashville and Davidson County.

Table of Contents

1 Overview.....	4
1.1 General Information.....	4
1.2 Schedule.....	4
1.3 Negotiation Controls.....	4
1.4 Terms.....	4
1.5 Attachments.....	4
2 Requirements.....	5
2.1 Section 1. RFP Solicitation (Selection) Method.....	5
2.2 Section 2. Waiver Process.....	6
2.3 Section 3. Commodity Codes.....	6
2.4 Section 4. Multi-Round Solicitation.....	7
2.5 Section 5. Timeline.....	7
2.6 Section 6. Solicitation Objective.....	8
2.7 Section 7. Scope Summary.....	8
2.8 Section 8. Scope Details.....	9
2.9 Section 9. Equal Business Opportunity (EBO) Program Requirements.....	120
2.10 Section 10. Insurance Requirements.....	120
2.11 Section 11. Standard Solicitation Requirements.....	121
2.12 Section 12. Information Security Agreement.....	128
2.13 Section 13. Solicitation Acceptance.....	129
2.14 Section 14. Contract Acceptance.....	129
2.15 Section 15. Evaluation Criteria.....	130
2.16 Section 16. Affidavits.....	157
3 Contract Terms.....	162

1 Overview

1.1 General Information

Title	Police Records Management System		
Amendment Date	6/11/2026 12:58 PM		
Amendment Description	Attached pre-offer meeting attendee sheet and powerpoint		
Buyer	Terri Lynn Ray	Outcome	Contract Purchase Agreement
E-Mail	Terri.Ray@nashville.gov		

1.2 Schedule

Preview Date		Open Date	6/11/2026 12:58 PM
Close Date	8/5/2026 2:00 PM	Award Date	
Time Zone	Central Standard Time		

1.3 Negotiation Controls

Response Visibility **Sealed**

1.4 Terms

Agreement Start Date		Agreement End Date	
Agreement Amount (USD)			
Payment Terms	Net 30	Freight Terms	SUPPLIER PREPAID
Shipping Method		FOB	DELIVERY
Negotiation Currency	USD (US Dollar)	Price Precision	0

1.5 Attachments

File Name or URL	Type	Description
IT Environment Requirements	File	

2 Requirements

**Response is required*

2.1 Section 1. RFP Solicitation (Selection) Method

1.

Request for Proposal

Pursuant to Metropolitan Code of Laws (M.C.L.) Section 4.12.040, this solicitation document serves as the written determination of the Purchasing Agent, that the use of competitive sealed bidding is neither practicable nor advantageous to Metro. Therefore, this solicitation will facilitate the entering into of contract (s) by the competitive sealed proposals process. The proposal process, flexibility and limitations are governed by the Code and related Procurement Regulations.

The proposal selection method permits discussions with offerors who submit proposals determined to be reasonably susceptible of being selected for award. Modifications in proposal content, comparative judgmental evaluations of the proposals, corrections, and scope adjustments, may occur at the request of the Purchasing Agent or their designee.

There may be one or more amendments to this solicitation. Solicitation amendments are included as updates to the original solicitation. It is the offeror's responsibility to remain informed on all solicitation amendments and submit the solicitation response incorporating all amendments.

Offers to Metro online solicitations are required to be submitted within the iSupplier online environment unless otherwise stated. Hard copy offers will not be considered except as required by law.

Any response to this solicitation is a formal waiver of any claims of confidentiality regardless of what may be stated, printed, or implied in the submission and/or attachments submitted. All information is made a Public Record after an award is made.

The only official position of Metro is found within this solicitation document including answers provided in response to questions raised. The online discussion tool within iSupplier is the appropriate tool for all questions or communications concerning this solicitation.

Metro reserves the right to issue additional rounds as it deems necessary for the purposes of evaluation. Additional rounds may include, but not be limited to, Offeror interviews.

Metro reserves the right to make multiple awards for a contract if it is deemed in the best interest of Metro.

2.2 Section 2. Waiver Process

1. Pursuant to Metropolitan Code of Laws (M.C.L.) Section 4.48.115 (Conflicts with Previous Metro Projects), Non-Metro employees who provide services to the metropolitan government regarding the feasibility, cost, design, implementation, or legislative adoption of a particular matter are prohibited from subsequent participation in the procurement process or resultant contract(s) related to that particular matter.

Any offeror who may meet the standard of MCL 4.48.115 must disclose this potential conflict to the buyer prior to the solicitation's deadline for questions. This disclosure must include reference to the offeror's prior work on the particular matter, including the specific project and prospective offerors' participation, and the timeframe services were rendered. If the offeror is requesting a waiver from MCL 4.48.115 this must be explicitly stated in the disclosure.

Requests for a waiver will be reviewed by the Procurement Standards Board with final decisions published in the news items section of purchasing.nashville.gov.

2.3 Section 3. Commodity Codes

1.
 - 43210000 - Computer Equipment and Accessories
 - 43230000 - Software
 - 46150000 - Law enforcement
 - 73170000 - Manufacture of electrical goods and precision instruments
 - 81110000 - Computer services
 - 81111503 - Systems integration design
 - 81111504 - Application programming services
 - 81112200 - Software maintenance and support
 - 83120000 - Information services
 - 92120000 - Security and personal safety

2.4 Section 4. Multi-Round Solicitation

1.

Solicitation Rounds

This is a multi-round solicitation that will consist of at least three (3) rounds. Metro reserves the right for additional rounds if deemed necessary.

Round 1

Round 1 consists of Experiences and Qualifications, RMS Implementation and Support, RMS Technical Overview, and RMS Modules for a total of 2000 Points. Offerors evaluated as qualified from Round 1 will be invited to the next round(s).

Round 2

Offerors evaluated as qualified from Round 1 will be invited to Round 2 wherein Offerors will have an opportunity to participate and respond to demonstrations for a total of 2500 Points. Offerors evaluated as qualified from Round 2 will be invited to the next round(s).

Round 3

Offerors evaluated as qualified from Round 2 will be invited to Round 3 wherein Offerors will have opportunity to submit cost for a total of 3000 Points.

Points from Round 1, 2, and 3 will be added together to determine who receives the max points (7500).

2.5 Section 5. Timeline

1.

The following is the general, unofficial anticipated timeline for this solicitation. These dates represent a good faith effort, accurate at the time of publication. They are non-binding and subject to change. They are for informational purposes only and subsidiary to official dates/times contained elsewhere in the solicitation:

- 06/03/2026 – Round 1 Solicitation Opens
- 06/10/2026 - Pre-Offer Meeting
- 06/11/2026 - Round 1 Amendment Published with Pre-Offer PowerPoint and Attendee List
- 06/24/2026 - Round 1 Deadline to Submit Questions in iSupplier
- 07/08/2026 - Round 1 Amendment Published with Response to Online Discussion Questions
- 08/05/2026 - Round 1 Solicitation Closes
- 08/11/2026 - Responsive Offers Provided to Evaluation Committee
- 09/21/2026 – 10/01/2026 - Evaluation Committee Meeting
- 10/14/2026 - Published Round 2 to shortlisted offerors
- 10/19/2026 - Round 2 Deadline to Submit Questions in iSupplier
- 10/22/2026 - Round 2 Amendment Published with Response to Online Discussion Questions
- 11/02/2026 – 01/15/2027– Round 2 Demonstration period
- 01/19/2027 - Round 2 Solicitation Closes
- 01/21/2027 - Responsive Offers Provided to Evaluation Committee
- 01/26/2027 - Evaluation Committee Meeting
- 02/02/2027 - Published Round 3 to shortlisted offerors
- 02/08/2027 - Round 3 Deadline to Submit Questions in iSupplier
- 02/11/2027 - Round 3 Amendment Published with Response to Online Discussion Questions
- 02/18/2027 – Round 3 Solicitation Closes
- 02/23/2027 - Evaluation Committee Meeting
- 03/02/2027 - Intent to Award Issued
- 03/12/2027 - Protest Period Ends & Deadline for Awarded Supplier to Provide Outstanding Documents
- 04/15/2027 – Finalized PDF of Contract Documents Sent to Awarded Supplier and Department for Review.
- 04/22/2027 - Contract Routes for Signatures, including Council Approval
- 06/30/2027 - Sourcing Process Complete

2.6 Section 6. Solicitation Objective

1. The objective of this solicitation is to enter into a Metro contract to provide a complete and fully functional Records Management System (RMS). The contract term is five (5) years, with two (2) optional two-year extensions and one (1) optional one-year extension.

2.7 Section 7. Scope Summary

1. The Metropolitan Government of Nashville and Davidson County (Metro) is soliciting proposals for a qualified Offeror to deliver a comprehensive Law Enforcement Records Management System (RMS) for the

Metropolitan Nashville Police Department (MNPd).

The proposed solution must fully support the operational needs of MNPd and its criminal justice partners per details outlined herein.

2.8 Section 8. Scope Details

1. MNPd Key RMS Details (numbers are approximate):

- RMS Implemented in: 2009
- Active MNPd RMS Users (past year): 1,027
- Total RMS Users: 3000
- External RMS Users: 184
- Total Partner Agencies: 16
- Annual User Connections: 149,756
- Average Daily RMS Connections: 4,831
- Database Size: 6.8 TB (predominantly documents and images)
- Database Platform: Oracle 19.19.0.0.0 on Oracle Server Release 7.9
- Configuration: Dual Oracle Data Appliances (ODA) in failover mode via Oracle Data Guard

MNPd Approximate Staffing (as of January 2026)

- Lieutenants: 99
- Sergeants: 336
- Officers: 1,079
- MNPD Trainees: 70
- Total Police Staffing: 1,636
- Budgeted Staffing for Police is 1,720
- Civilian Support Staff: 508

Average Response Metrics (as of January 2026):

- Average Response Time: 12.8 minutes
- Average Queue Time: 4.4 minutes
- Average Travel Time: 8.4 minutes

Attachments:

File Name or URL	Type	Description
Acronym Term Glossary.pdf	File	

2. GENERAL PROVISIONS

1. RMS Requirements

1.a. The RMS must support the full lifecycle of data from initial call-for-service through incident reporting, investigations, citations, arrests, evidence management, case closure, and data analytics. The RMS should promote transparency, efficiency, officer safety, accountability, and community trust. The RMS must be capable of integration with internal systems, external agencies, and national databases outlined herein while maintaining compliance with all applicable legal, privacy, and security standards.

1.b. Awarded offeror should be prepared to conduct a detailed discovery and analysis phase to evaluate MNPD's existing RMS to ensure continuity of all current MNPD RMS Interfaces upon contract execution.

1.c. MNPD will provide timely access to subject matter experts, IT staff, and end users for the Offeror's current RMS functionality gathering and for testing new processes.

1.d. All project activities will be conducted within agreed timelines, with both parties responsible for meeting their commitments.

1.e. The RMS solution must support the full migration of data from the current RMS to the new RMS, ensuring accuracy, integrity, and minimal disruption to operations.

1.f. The RMS should allow administrators to manage configuration changes, version control, user role adjustments, and permissions without the need for Offeror support in day-to-day operations.

2.Communication

2.a. The Offeror is required to provide effective communication throughout the contract life. Effective communication is essential to ensuring project alignment, timely decision-making, risk mitigation, and overall project success.

2.b. Offeror must ensure transparency, traceability, and effective communication regarding software updates and modifications to the Records Management RMS. The Offeror shall produce and deliver comprehensive Software Release Notes to the Customer for every software release, update, patch, or modification to the Records Management System, whether major or minor. The Release Notes shall include at a minimum the following:

2.b.1. Version Identification: Clear version number and release date.

2.b.2. Summary of Changes: Description of new features, enhancements, bug fixes, and performance improvements.

2.b.3. Defect Resolution: Identification of issues corrected, including reference numbers where applicable.

2.b.4. Known Issues: Any unresolved defects or limitations remaining in the release.

2.b.5. Impact Assessment: Description of any functional, data, configuration, or user interface impacts.

2.b.6. Installation or Upgrade Instructions: Steps or prerequisites required for implementing the release.

2.b.7. Dependencies: Identification of any changes to hardware, software, or third-party components.

2.b.8. Backward Compatibility: Statement indicating whether backward compatibility is maintained.

2.b.9. Delivery: Release Notes shall be delivered to the Customer at least ten (10) business days prior to implementation in electronic (PDF or Word) formats.

2.b.10. Archive: The Offeror should maintain a cumulative archive of all Release Notes and make them available to the Customer upon request.

2.c. Failure to provide complete and accurate Release Notes may delay acceptance of the software release or result in rejection of the update until documentation requirements are fulfilled.

3. Accreditation

3.a. The RMS must support compliance with federal, TN, and local accreditation standards, including but not limited to CALEA (Commission on Accreditation for Law Enforcement Agencies), FBI NIBRS and Standards, CJIS Standards, and Tennessee Incident-Based Reporting System (TIBRS) and Standards (website links included in attachment section herein).

3.b. The RMS should include built-in tools for auditing, compliance tracking, and documentation of accreditation-related policies and procedures.

4. Open Architecture

4.a. The RMS must be based on an open architecture that enables integration with third-party systems via standardized APIs and data exchange protocols. The RMS should not rely on proprietary technologies that restrict integration, scalability, or interoperability with evolving law enforcement tools and platforms.

4.b. Offeror shall ensure all system components interoperate with MNPd's existing and future systems using non-proprietary, industry-standard protocols and data formats (e.g., JSON, XML, NIEM, CJIS-compliant formats). Offeror may not impose contractual, technical, or financial barriers that restrict MNPd from integrating third-party systems.

4.c. The Offeror shall provide third-party integrators with: API credential information, documentation, test environments, and reasonable technical support as needed to complete integrations.

4.d. Offeror shall supply MNPd with fully documented, versioned, industry standards-based APIs. APIs must be accessible throughout the contract term without additional fees other than those explicitly defined in the contracted pricing schedule. Offeror shall provide at least 90 days' written notice before any deprecation, modification, or retirement of an API, and shall maintain backward compatibility for no fewer than 180 days.

4.e. Offeror must ensure that APIs support real-time, secure, and performant access consistent with reasonable SLA metrics. API limits, if there are any, must be transparent, reasonable, and not inhibit system interoperability.

4.f. Offeror may update APIs but may not impose changes that break existing integrations without providing migration guidance, test sandboxes, and adequate transition periods.

5. System Environments

5.a. The RMS should operate in secure, redundant environments that support high availability, disaster recovery, and business continuity. It should be compatible with modern IT environments, including, but not limited to:

5.a.1. Microsoft Windows and Active Directory

5.a.2. Cloud services (AWS, Azure, GovCloud)

5.a.3. Web-based and thin-client deployments

5.a.4. Mobile-first design principles

5.a.5. iOS 26.4.2 or greater on iPhone 15

6. Data Sharing

6.a. The RMS must enable controlled and auditable data sharing across agencies, jurisdictions, and partner organizations. Support is required for:

- 6.a.1. Inter-agency data sharing agreements
- 6.a.2. Regional crime data exchanges
- 6.a.3. Multi-agency task force collaboration
- 6.a.4. Customizable access permissions based on user roles and legal requirements

7. Identity Management

7.a. The RMS should support enterprise-level identity management using industry standards such as:

- 7.a.1. Single Sign-On (SSO)
- 7.a.2. Microsoft Active Directory/Microsoft Entra ID integration
- 7.a.3. Multi-Factor Authentication (MFA)
- 7.a.4. Role-Based Access Control (RBAC)

7.b. All modules and Core Components must implement Role-Based Access Control (RBAC), allowing administrators to define roles based on job functions or assignments.

7.c. Roles should define access to specific modules, data fields, or actions (e.g., view, create, edit, delete, export).

7.d. Users may be assigned multiple roles, and the module should resolve permissions logically based on most restrictive or most permissive rules as configured.

7.e. The module should allow for the creation of custom roles and template roles for rapid onboarding.

7.f. Roles should be assignable at the individual, group, unit, or agency level.

7.g. The RMS should restrict sensitive asset information (e.g., tactical equipment) to authorized roles.

7.h. Restrict access to audit logs to authorized administrative or supervisory roles.

7.i. Prevent modification, suppression, or deletion of any audit data by any user, including system administrators.

7.j. Support audit trails for access to the audit logs themselves.

7.k. The RMS must log all access attempts, modifications, and user activity for audit purposes.

8. Cross-Module Functionality

8.a. The RMS must provide seamless integration and data sharing across all modules and core components, including case management, arrest, evidence, traffic, and citations. A single data entry point should populate all relevant modules, eliminate duplication and ensure data consistency. Modules should be natively connected to support holistic workflows.

9. Configurability

9.a. The RMS must be highly configurable to meet the evolving operational needs of MNPd. MNPd should be able to modify:

- 9.a.1. Field labels and picklists
- 9.a.2. Workflows and approval chains
- 9.a.3. Notification rules and escalation triggers
- 9.a.4. User roles and permissions
- 9.a.5. System Configuration (e.g. Web Services, SMTP, SFTP)

9.b. All configuration tools should be accessible to RMS administrators without requiring the offeror's assistance for routine changes.

10. Attachments

10.a. The RMS must support attaching various file types (e.g., PDFs, XPS, images, audio, video, scanned documents) to any record within the RMS. Attachment functionality should include:

- 10.a.1. Drag-and-drop image upload
- 10.a.2. Metadata tagging and descriptions
- 10.a.3. Audit logs for upload/view/download

10.b. Support for cloud-based storage or direct integration with evidence management systems.

11. Automated Notifications

11.a. The RMS should support configurable automated notifications triggered by specific actions, timeframes, or record status changes. Notifications may be delivered via:

- 11.a.1. In-system alerts
- 11.a.2. Email or SMS (group)
- 11.a.3. Task assignment dashboards

11.b. Examples include supervisor approval requests, court date reminders, warrant follow-up, or overdue report notifications.

12. Searchability

12.a. The RMS must provide powerful search capabilities across all modules, including, but not limited to:

- 12.a.1. Global search from a single interface.
- 12.a.2. Advanced filtering by date range, location, officer, incident type, or keyword.
- 12.a.3. Full-text search of narrative reports and attachments.

12.a.4. Saved searches and custom query templates for users.

13. Printing

13.a. The RMS must support secure, on-demand printing of reports, citations, case files, and attachments. Features should include:

13.a.1. Batch printing

13.a.2. Cover Page

13.a.3. Document Footer Options:

13.a.3a. Document Name

13.a.3b. Date document printed

13.a.3c. Page Number

13.a.3d. Page Number of Total Pages (e.g., Page 14 of 21)

13.a.4. Editable text

13.a.5. Watermarking (e.g., "Draft," "Confidential", "Do Not Print or Copy", or editable text)

13.a.6. Exporting formats including, but not limited to: PDF and XPS

14. Mobile Technology

14.a. The RMS must include a mobile-responsive interface or dedicated mobile application for officers and investigators in the field. iPhone use of RMS is of particular importance for MNPD. A Native iOS app is to a Web app. Mobile functionality should include, but not limited to:

14.a.1. Report writing

14.a.2. Person and vehicle queries

14.a.3. Attachment uploads (photos, audio, etc.)

14.a.4. Signature capture

14.a.5. Offline mode with sync upon reconnection.

14.b. The mobile platform must be compatible with iOS smartphones (iPhone 15 with iOS 26.4.2 or greater), and Windows 11 based-tablets.

15. Organizational Environment

15.a. Users will have access to standard computing devices (desktops, laptops, tablets, and/or mobile devices) with reliable internet connections.

16. Records Management

16.a. The RMS will manage both physical and electronic records, including structured and unstructured

content.

16.b. Integration with existing systems and their expected growth will be required as are identified in the RFP.

16.c. RMS data estimates provided in the RFP (number of users, database size, etc.) are accurate within a reasonable margin.

16.d. The RMS solution must include the development of connections between all current MNPd interfaces to enable secure and efficient data exchange between MNPd and various criminal justice agencies.

17. Data & Security

17.a. MNPd will have sole ownership of all data stored in the RMS. MNPd Data cannot be sold or used without express written approval from MNPd.

17.b. The RMS offeror must comply with applicable data protection, privacy, and security regulations (e.g., CJIS, NIBRS/TIBRS, HIPAA) during the contract term.

17.c. The RMS offeror accepts responsibility for maintaining security patches and system updates during the contract term.

18. Common Output Options

18.a. The following list of output options are acceptable for the RMS:

- 18.a.1. CSV (Comma-Separated Values)
- 18.a.2. DOCX - DOC (Microsoft Word)
- 18.a.3. HTML (Web Viewable Reports)
- 18.a.4. JSON (JavaScript Object Notation)
- 18.a.5. PDF (Portable Document Format)
- 18.a.6. RTF (Rich Text Format)
- 18.a.7. TXT (Plain Text)
- 18.a.8. XML (Extensible Markup Language)
- 18.a.9. XPS (XML Paper Specification) – required with a current MNPd RMS Interface.
- 18.a.10. XLSX (Microsoft Excel)

19. Future Scalability and Advancement

19.a. The RMS must be able to scale in terms of users, storage, and functionality without requiring complete reimplementations and resolved within acceptable timelines.

19.b. Upgrades, patches, and version releases will not disrupt business continuity when performed according to offeror's best practices.

19.c. Ongoing support and maintenance requirements will be addressed as part of the service level

agreement (SLA). Per the contract exception language, offerors are required to submit a copy of the service level agreement for Metro's review.

19.d. Upon request offeror must provide MNPd Data in a complete, non-proprietary, and documented data format upon request, at any time and for any reason, without penalty and within a reasonable time. Offeror must provide all necessary metadata, schema documentation, and configuration details required for reconstruction.

20. Legal and Regulatory Compliance Monitoring

20.a. The selected offeror shall be responsible for proactively monitoring, identifying, and implementing all necessary updates or modifications to the Records Management System (RMS) to ensure ongoing compliance with all applicable local, TN, and Federal laws, as well as any changes or updates to National Incident-Based Reporting System (NIBRS) and Tennessee Incident-Based Reporting System (TIBRS) standards and requirements. This includes, but is not limited to:

20.a.1. Tracking and interpreting legislative or regulatory changes that impact law enforcement reporting or data management.

20.a.2. Updating RMS functionality, forms, data fields, reporting outputs, or validation rules in response to changes in statutory or regulatory requirements.

20.a.3. NIBRS and TIBRS code and requirement changes

20.a.4. Ensuring timely implementation of updates to maintain compliance without disruption to MNPd operations.

20.a.5. Providing documentation and user communication related to any such changes.

20.a.6. Failure to maintain compliance due to lack of timely updates shall be the sole responsibility of the offeror.

Attachments:

File Name or URL	Type	Description
Tennessee Incident-Based Reporting System (TIBRS) and Standards	URL	
CJIS Standards	URL	
FBI NIBRS and Standards	URL	
CALEA (Commission on Accreditation for Law Enforcement Agencies)	URL	

3. 21. RMS Hosting Platform

21.a. The Records Management System (RMS) shall support deployment in cloud, on-premises, or hybrid hosting environments. MNPd prefers that the RMS shall provide hybrid architecture options, including but not limited to:

21.a.1. Real-time synchronization of RMS data to an on-premises data lake

21.a.2. A fully hybrid configuration with applications and/or data hosted both on-premises and in the cloud

21.a.3. Secure bidirectional data exchange between environments

21.b. The RMS shall support dynamic scalability to accommodate changes in operational demand, including:

21.b.1. Increasing numbers of users and sites

21.b.2. Growth in data volume and transaction load

21.b.3. Horizontal and/or vertical scaling

21.c. The RMS shall provide monitoring and alerting capabilities for system health and connectivity, including:

21.c.1. Failed connections

21.c.2. Latency issues

21.c.3. Bandwidth spikes

21.c.4. Service interruptions

21.d. The RMS shall be deployable in geographically separated U.S. data centers.

21.e. The RMS shall be CJIS compliant.

21.f. The RMS shall allow MNPDP unrestricted access to customer-owned data via system interfaces, including APIs, without limitations or additional fees for:

21.f.1. Data access

21.f.2. Data transfer

21.f.3. Data export or download

21.f.4. Integration with third-party systems

21.g. The RMS shall support high availability and disaster recovery appropriate for mission-critical public safety operations.

21.h. MNPDP retains full ownership of all MNPDP Data, including metadata and derivative data. Offeror shall obtain no rights in MNPDP Data except those explicitly granted for the sole purpose of delivering services. Offeror shall not access, use, analyze, mine, or disclose MNPDP Data for any secondary purpose, including analytics, product development, advertising, training of AI models, or data monetization, without express written consent.

22. RMS Data Quality Attributes

22.a. The RMS shall maintain high-quality data characteristics to ensure operational effectiveness, regulatory compliance, and long-term sustainability.

22.b. The RMS shall support operation across multiple environments and platforms, including:

22.b.1. On-premises and cloud hosting options

22.b.2. Data portability between environments

- 22.b.3. Access via desktop, web, and mobile interfaces
- 22.c. The RMS shall support efficient system testing, including:
 - 22.c.1. Built-in quality assurance or validation tools
 - 22.c.2. Support for automated testing processes
 - 22.c.3. Test environments that mirror production functionality
- 22.d. The RMS shall accommodate growth without degradation in performance in:
 - 22.d.1. User volume
 - 22.d.2. Transaction load
 - 22.d.3. Data storage
- 22.e. The RMS shall support efficient maintenance, including:
 - 22.e.1. Application of updates and patches
 - 22.e.2. Modular architecture
 - 22.e.3. Clear system documentation
 - 22.e.4. Vendor support for enhancements and changes
- 22.f. The RMS shall integrate with external systems and data sources, including support for:
 - 22.f.1. Industry standards such as NIEM, CJIS, UCR, NIBRS, and TIBRS
 - 22.f.2. APIs and data exchange mechanisms
 - 22.f.3. Interfaces with third-party public safety systems
- 22.g. The RMS shall provide consistent and responsive performance under operational conditions, including high system availability.
- 22.h. Authorized users shall be able to access and retrieve records quickly and efficiently.
- 22.i. The RMS shall support internal and external audits, demonstrating data accountability, governance, and traceability.

23. RMS Data Cleansing, Merge, Migration and Conversion Approach

- 23.a. The RMS shall provide automated data duplication detection, cleansing, and record merge capabilities to ensure accuracy, integrity, and consistency across all system records.
- 23.b. The RMS shall identify potential duplicate records across applicable data domains, including but not limited to:
 - 23.b.1. Persons
 - 23.b.2. Vehicles

23.b.3. Properties/locations

23.b.4. Incidents, cases, and reports

23.b.5. Evidence and related entities

23.c. The RMS shall support duplicate detection through:

23.c.1. Real-time checks during data entry

23.c.2. Scheduled batch processing

23.c.3. On-demand data quality scans

23.d. The RMS shall provide configurable matching criteria, including, but not limited to:

23.d.1. Exact matches

23.d.2. Partial or fuzzy matches

23.d.3. Multi-field matching

23.e. The RMS shall allow authorized users to review, confirm, merge, or dismiss duplicate records prior to permanent changes.

23.f. The RMS shall maintain a complete audit trail of duplication detection and cleansing activities, including:

23.f.1. User identification

23.f.2. Date and time

23.f.3. Actions taken

23.f.4. Details of modified or merged records

23.g. The RMS shall support record merging with user control over:

23.g.1. Selection of a master record

23.g.2. Field-level data retention

23.g.3. Preservation of relationships and references

23.h. The RMS shall ensure that merging actions do not compromise:

23.h.1. Data integrity

23.h.2. Reporting accuracy

23.h.3. Evidentiary chain of custody

23.i. The RMS shall provide rollback or recovery options for merged records, subject to administrative permissions.

23.j. The RMS may include AI or machine-learning assisted features, such as:

- 23.j.1. Intelligent duplicate detection based on contextual similarity and historical patterns.
- 23.j.2. Confidence scoring indicating the likelihood that records are duplicates.
- 23.j.3. Automated recommendations for merge candidates and master records.
- 23.j.4. Adaptive learning based on user decisions.
- 23.j.5. Analysis of unstructured or narrative data to identify potential duplicates.

23.k. The RMS shall provide administrative dashboards and reports showing:

- 23.k.1. Duplicate detection activity
- 23.k.2. Data quality trends
- 23.k.3. Cleansing outcomes

23.l. The RMS shall allow administrators to configure:

- 23.l.1. Matching rules
- 23.l.2. Thresholds
- 23.l.3. AI sensitivity levels (if applicable)

4.

RMS Modules

The proposed RMS solution should include the following modules as detailed herein.

24. Arrest/Booking Integration Module

24.a. The RMS should include a robust, fully integrated Arrest/Booking Management Module to MNPD in processing and managing arrested individuals. The module should:

- 24.a.1. Be compliant with local, TN, and federal standards and reporting requirements.

24.a.2. Support both pre-booking and post-booking data entry workflows.

24.a.3. Be integrated with other RMS modules including Incident, Arrest, Warrants, Property and Evidence, and Case Management.

24.a.4. Support MNPd configurable workflows, business rules, and user permissions.

24.b. The management intake functions of the module should provide the ability to:

24.b.1. Create a new booking record from an arrest or warrant.

24.b.2. Capture and validate arrestee biographical data including name, aliases, DOB, gender, race, ethnicity, address, physical descriptors, scars/marks/tattoos, and identifiers (e.g., SSN, driver's license, passport number, state ID, FBI/CJIS numbers).

24.b.3. Link arrestees to known persons or prior booking/arrest records.

24.b.4. Record and manage multiple charges per booking event, with the ability to link charges to statutes.

24.b.5. Allow manual or automated entry of booking date and time.

24.b.6. Flag individuals with special conditions (e.g., medical, suicidal, violent, gang affiliation).

24.b.7. Support duplicate checking to prevent redundant records.

24.b.8. Support integration with digital imaging systems for mugshots (front, profile, and other views) – DataWorks Plus Version 5.165

24.b.9. Allow photo tagging (e.g., scars, injuries, tattoos).

24.b.10. Integrate with NEC AFIS Live Scan fingerprint systems.

24.b.11. Provide audit trails of all biometric data collection.

24.b.12. Maintain a full chronological record of all Arrest/Booking Management-related activities.

24.b.13. Accept intake times, changes to charges, housing changes, property check-ins/outs, medical interventions, and releases received via DCSO JIS interfaces..

24.b.14. Support time-based reporting of Arrest and Booking module.

24.b.15. Integrate with CAD, DCSO Jail Management Systems, Davidson County Court Systems, Juvenile Court Systems, NEC AFIS, and DataWorks Plus Version 5.165 Mugshots.

24.b.16. Interface with state and federal systems for warrant checks, fingerprint submission, and criminal history retrieval.

24.b.17. Support electronic transmission of Arrest/Booking Management data to TN Criminal History repositories and NCIC/Nlets.

24.b.18. Provide standard Arrest/Booking Management reports (e.g., daily intake, demographic statistics, charge summaries).

24.b.19. Support ad hoc reporting with user-defined fields and filters.

24.b.20. Maintain audit logs of all data changes, including user ID, timestamp, and nature of change.

24.b.21. Restrict access to juvenile records, medical/mental health information, and sealed charges.

24.b.22. Support detailed user permissions for booking intake, modification, and expungement for external agencies.

24.b.23. Ability to attach documents (e.g., arrest reports, court orders).

24.b.24. Ability to generate and print booking packets or summaries.

24.b.25. Module should support undo/void functionality with full audit trail.

24.b.26. Module has the capability to populate booking forms electronically.

24.b.27. Module has the capability to accept pre-booking information electronically from field-based reporting.

24.b.28. Module has the capability to transfer the pre-booking data to the DCSO Jail Management System, NEC, DWP, CJIS, and Quest JIMS.

24.b.29. Module displays a warning or notification when a person of interest is booked.

24.b.30. Module documents different booking data based on whether booking for juveniles or adults.

24.b.31. Module creates/updates the Master Name Index (MNI) when creating, modifying, or deleting a booking.

24.b.32. Module automatically checks against the Master Name Index when creating or modifying a booking.

24.b.33. All supplemental reports are linked to the original incident report. MNPD should be able to link all associated reports to a common report number.

24.b.34. Module should support a real-time warrant check.

24.b.35. Module should support court date scheduling and notifications.

24.b.36. Module should support transport and holding log.

24.b.37. While active in the Booking module, authorized users have access to arrest details, and other prior records.

24.b.38. Photo images can be uploaded from DataWorks Plus Photo Manager - Version 5.165

25. Asset Management Module

25.a. The RMS should allow authorized personnel to register new assets (e.g., firearms, radios, vehicles, body cameras, uniforms).

25.b. The RMS should support categorization of assets (e.g., equipment, electronics, vehicles, and weapons).

25.c. The RMS should allow attachment of supporting documentation (e.g., purchase receipts, warranties, manuals).

25.d. The RMS should assign a unique asset ID or barcode (Code 39)/QR code to each asset.

25.e. The RMS should support bulk asset import via CSV or integration API.

25.f. The RMS should allow assets to be assigned to officers, departments, or units.

25.g. The RMS should record the date, time, and person responsible for each assignment or reassignment.

25.h. The RMS should track the location of assets (e.g., headquarters, precinct, vehicle, off-site storage).

25.i. The RMS should allow for scheduled and ad-hoc audits or inventories.

25.j. The RMS should maintain a full audit trail of all asset transactions and status changes.

25.k. The RMS should record user ID, timestamp, and action for each asset event.

25.l. The RMS should allow for electronic and digital signatures for sensitive asset transfers (e.g., firearms, evidence kits).

25.m. The RMS should track lifecycle stages (e.g., In Service, Under Repair, Lost, Retired, Sent to Surplus).

25.n. The RMS should support scheduled maintenance tracking with alerts and service-history logs.

25.o. The RMS should allow assets to be marked as decommissioned or disposed of with appropriate justification.

25.p. The RMS should generate reports on asset inventory, location, status, assignment history, and maintenance.

25.q. The RMS should provide low-inventory alerts (e.g., consumables or expendables).

25.r. The RMS should allow configurable alerts for maintenance, reassignment, or audits.

25.s. The Asset Management Module should integrate with Personnel, Case Management, and Evidence Management modules where applicable.

25.t. The RMS should update personnel profiles with assigned assets and equipment.

25.u. The Evidence Management module should notify the Asset Management module when an MNPd assigned asset is used in an incident or case, for example a recovered, stolen MNPd asset.

25.v. The RMS should retain asset transaction logs for a configurable period of time.

25.w. The RMS should generate compliance reports for internal audits and external regulatory inspections.

25.x. Integration with RFID/barcode/QR Code scanners for fast asset check-in/out.

25.y. Mobile app for field officers to view and manage assigned assets.

5. **26. Audit Trails and Access Logs Module**

26.a. The proposed RMS should include a comprehensive and tamper-proof Audit Trails and Access Logs Module that ensures all user activity within the RMS is recorded, traceable, and reviewable. This module should support internal oversight, security compliance, forensic investigation, and data integrity verification in accordance with local, TN, and federal regulations (e.g., CJIS Security Policy v6.0).

26.b. The Audit Trails and Access Logs Module should:

26.b.1. Automatically log all user actions within the RMS, including but not limited to:

- 26.b.1a. Record creation, viewing, editing, and deletion
- 26.b.1b. User logins/logouts (successful and failed)
- 26.b.1c. Report approvals, rejections, or workflow actions
- 26.b.1d. Data exports, print commands, and document downloads
- 26.b.1e. Changes to user accounts, permissions, and roles
- 26.b.1f. RMS configuration changes

26.b.2. Maintain a chronological, immutable log of events with:

- 26.b.2a. Timestamp (to the second, synchronized via system clock or NTP)
- 26.b.2b. User ID and role
- 26.b.2c. IP address or device ID (if available)
- 26.b.2d. Module or feature accessed
- 26.b.2e. Description of the action taken

26.b.3. Before/after values for edited records (field-level detail)

26.b.4. Capture both successful and failed attempts to access restricted data or features.

26.c. Provide advanced search and filtering tools for audit data based on:

- 26.c.1. User ID or name
- 26.c.2. Date and time range
- 26.c.3. Specific action or event type
- 26.c.4. Affected module or data type (e.g., case report, evidence, arrest)
- 26.c.5. IP address or workstation identifier
- 26.c.6. Allow audit logs to be exported to standard formats (e.g., PDF, Excel, CSV) for internal and external auditing.
- 26.c.7. Support drill-down from data records (e.g., case files) to view complete access history for that item.

26.d. Allow configuration of real-time alerts for:

- 26.d.1. Unauthorized access attempts
- 26.d.2. After-hours access or abnormal user behavior

26.d.3. Large data exports or mass record views

26.d.4. Access to sensitive records (e.g., internal affairs, juvenile, sealed cases)

26.d.5. Provide administrative dashboards showing:

26.d.5a. Top accessed records – top users by access volume

26.d.5b. Recent login failures or lockouts

26.d.5c. Allow agencies to define audit log retention schedules in compliance with TN and federal mandates.

26.d.5d. Ensure audit logs are stored securely and are not alterable or able to be deleted by end users or administrators.

26.d.5e. Support the archiving of older logs while maintaining accessibility for audits and investigations.

26.e. The module should support compliance with:

26.e.1. Criminal Justice Information Services (CJIS) Security Policy v6.0

26.e.2. 28 CFR Part 23 (for intelligence systems)

26.e.3. TN-specific auditing and retention laws

26.e.4. HIPAA (if the RMS handles health-related data)

26.e.5. Integrate with all core RMS modules including, but not limited to:

26.e.5a. Case Reports

26.e.5b. Arrests/Warrants

26.e.5c. Evidence Management

26.e.5d. Field Interviews

26.e.5e. Other

26.f. Support high availability, backup, and disaster recovery for audit data.

26.g. Provide a user-friendly interface for authorized users to:

26.g.1. Search and review logs

26.g.2. Generate standard audit reports

26.g.3. Schedule recurring audit exports or alerts

26.h. Support API access for external auditing or SIEM systems (Security Information and Event Management), if applicable.

- 26.i. Store all audit and access logs in a separate, secure, tamper-evident database.
- 26.j. Encrypt audit logs at rest and in transit.
- 26.k. Ensure system clocks are synchronized using NTP or similar protocol to maintain accurate timestamps.

27. Be On the LookOut (BOLO) Module

- 27.a. The RMS should include a comprehensive BOLO (Be On the LookOut) Module that allows authorized personnel to create, update, manage, and disseminate information related to BOLOs and active hot warrants for both persons and vehicles. This module should support time-sensitive data entry, robust alerting, and MNPD-wide access to promote officer safety and situational awareness.
- 27.b. The RMS should provide a dedicated BOLO Module that is integrated with the Master Person Index and Master Vehicle Index.
- 27.c. The RMS should support the entry, management, and querying of BOLOs for persons, vehicles, and other items (e.g., stolen property, weapons).
- 27.d. The module should distinguish between BOLOs, hot warrants, informational alerts and AM Messages.
- 27.e. Each BOLO or hot warrant entry should have a unique identifier for tracking and auditing.
- 27.f. BOLOs should be linkable to other records in the RMS, including incidents, arrests, field interviews, and case files.
- 27.g. Users should be able to classify a BOLO by type (e.g., felony warrant, stolen vehicle, missing person, wanted for questioning, officer safety alert).
- 27.h. The module should allow priority levels (e.g., critical, high, moderate, informational) to be assigned to each BOLO.
- 27.i. Each BOLO should include both effective and expiration dates/times, after which the BOLO is deactivated automatically or by administrator review.
- 27.j. The module should allow entry of free-text narratives, physical descriptions, associated persons/vehicles, and photographs.
- 27.k. Users should be able to attach documents, images, or video files (e.g., surveillance footage) to a BOLO.
- 27.l. The module should support the creation and flagging of hot warrants associated with individuals and vehicles.
- 27.m. Hot warrants should be linked to relevant warrant records within the RMS or external warrant systems if integrated.
- 27.n. The module should clearly flag any BOLO that involves an active felony or extraditable warrant.
- 27.o. The module should provide real-time alerts for hot warrants when a matching person or vehicle is queried or entered in any RMS component.

- 27.p. The module should include visual indicators (e.g., red banners, bold icons) to identify hot warrant BOLOs in all search results and reports.
- 27.q. The module should support BOLOs for vehicles by license plate, VIN, make, model, color, and distinguishing features.
- 27.r. Users should be able to link vehicle BOLOs to known operators or persons of interest.
- 27.s. Vehicle BOLOs should support entries for stolen vehicles, suspect vehicles, vehicles of interest, or lookout alerts.
- 27.t. The module should allow for NCIC/State stolen vehicle status to be queried or synced when applicable.
- 27.u. Vehicle BOLOs should display images of the vehicle (if available) and support notation of modifications or damage.
- 27.v. The module should support advanced search functionality for BOLOs using name, alias, DOB, gender, race, physical descriptors, license plate, vehicle characteristics, location, date, type, and priority.
- 27.w. The module should allow wildcard and partial match searching (e.g., partial plate or alias name).
- 27.x. BOLOs should be searchable by geographic region, division, or assigned jurisdiction.
- 27.y. Users should be able to view a chronological list of all active and inactive BOLOs with filtering by status, priority, and type.
- 27.z. The module should generate real-time alerts when a person or vehicle matches an active BOLO or hot warrant.
- 27.aa. Alerts should appear in RMS modules including but not limited to Court Documents and Warrants, Incident, Arrest, Field Interview, Booking, and Master Index queries.
- 27.ab. The module should support configurable notifications via email, RMS inbox, mobile alert, or CAD integration (if applicable).
- 27.ac. Alerts should include configurable acknowledgment and tracking (e.g., who viewed, when, and what action was taken).
- 27.ad. Officer safety flags and BOLO alerts should be presented prior to printing or generating reports involving the subject.
- 27.ae. The module should allow geotagging of BOLOs to associate them with last known locations or areas of interest.
- 27.af. Users should be able to view BOLOs on a map interface within the RMS, highlighting geographic patterns or clusters.
- 27.ag. The module should support geographic filtering (e.g., "show all BOLOs within two (2) miles of a specified location").
- 27.ah. The module should allow spatial alerts when entering or responding to a location associated with an active BOLO.
- 27.ai. Only authorized personnel should be allowed to create, modify, or deactivate BOLOs.

- 27.aj. The module should audit all BOLO creation, modification, view, and deletion activities.
- 27.ak. The module should restrict access to sealed or sensitive BOLOs based on clearance levels.
- 27.al. BOLOs should include expiration dates and automatic deactivation unless renewed.
- 27.am. The module should provide automated reminders for review of active BOLOs approaching expiration.
- 27.an. Users with appropriate permissions should be able to archive or deactivate BOLOs manually.
- 27.ao. Historical BOLOs should remain searchable and include timestamps for all lifecycle events (created, modified, deactivated).
- 27.ap. The module should support reporting on active, expired, and deactivated BOLOs by type, status, subject, location, and officer.
- 27.aq. Users should be able to generate summary statistics for BOLOs over time, including types issued, frequency, and resolution outcomes.
- 27.ar. The module should support exporting of BOLO data for briefing packets, roll call reports, or tactical bulletins.
- 27.as. The module should include a dashboard or widget to show active BOLOs by region or category.
- 27.at. The BOLO Module should integrate with the RMS Master Person and Master Vehicle Modules.
- 27.au. The module should support NCIC/NLETS queries and updates for persons or stolen vehicles.
- 27.av. The module should be capable of sharing BOLOs with neighboring jurisdictions or regional information-sharing systems.
- 27.aw. The BOLO Module should support data exchange via standard APIs or secure messaging protocols.
- 27.ax. MNPD is currently using their BOLO module for Warrant Deconfliction.

6. **28. Case Management Module**

- 28.a. The module should allow authorized users to create new cases with unique case identifiers.
- 28.b. The module should auto-populate certain case fields (e.g., date/time, location) based on incident reports or dispatch data.
- 28.c. The module should support manual and automatic assignment of cases to officers, detectives, or units and provide information about prior involvement.
- 28.d. The module should allow reassignment of cases with audit tracking.
- 28.e. The module should support classification of cases by type (e.g., homicide, theft, assault).
- 28.f. The module should allow custom case categories and sub-categories to be defined by administrators.
- 28.g. The module should track and display investigative case statuses (e.g., Open, Active, Suspended, Closed, Unfounded).

- 28.h. The module should allow users to update status with required justification or notes.
- 28.i. The module should log all status changes with time stamps and user identification.
- 28.j. The module should allow authorized users to enter detailed case notes and narratives.
- 28.k. The module should support rich text formatting and templated reports.
- 28.l. The module should allow for cut and paste, plain and formatted text entry.
- 28.m. The module should allow users to upload and attach documents and images, and link to videos, audio recordings, and other digital evidence to the Incident module.
- 28.n. All notes and attachments should be time-stamped and associated with the user who entered them.
- 28.o. The module should allow the creation of tasks related to case investigation.
- 28.p. Tasks can be assigned to individuals or groups, with due dates and priority levels.
- 28.q. The module should send notifications and reminders for upcoming or overdue tasks.
- 28.r. Task completion should be tracked and auditable.
- 28.s. The module should provide visual and/or tabular relationship views.
- 28.t. The module should support many-to-many relationships and update changes dynamically.
- 28.u. The module should integrate with the Evidence and Property module.
- 28.v. Evidence items should be viewable and searchable within the case file.
- 28.w. The module should provide predefined case summaries and detailed reports.
- 28.x. Users should be able to filter cases by status, type, assigned personnel, dates, etc.
- 28.y. The module should support generation of investigative timelines.
- 28.z. The module should support exporting case data to PDF, Word, or Excel and may support other formats.
- 28.aa. The module should integrate with existing report-generating programs (e.g., Power BI)
- 28.ab. All changes to case records should be logged in an audit trail.
- 28.ac. The audit trail should include time, date, user ID, and change details.
- 28.ad. The module should be compliant with CJIS and MNPd retention rules.
- 28.ae. Sensitive cases (e.g., internal affairs, juvenile) should have additional access restrictions.
- 28.af. Supervisors should have override or administrative access for case review.
- 28.ag. Supervisors and assigned detectives should have ability to assign access for case review by outside agencies.

- 28.ah. Supervisors should have the ability to assign additional personnel for access.
- 28.ai. The module should support customizable workflows (e.g., supervisor approval of case closure, alerts).
- 28.aj. Users should be notified of pending reviews or actions required.
- 28.ak. The module should support approval queues with status indicators.
- 28.al. The module should integrate with:
 - 28.al.1. Computer-Aided Dispatch (CAD) system
 - 28.al.2. Master Name Index (MNI)
 - 28.al.3. Evidence Management
 - 28.al.4. DCSO Jail Management System
 - 28.al.5. Incident Module
 - 28.al.6. Accident Module
 - 28.al.7. Adult and Juvenile Court Document and Warrant Module
 - 28.al.8. Adult and Juvenile Arrest module
- 28.am. The module should include Case Prep functionality that allows authorized users to generate a comprehensive file of all documents and images associated with a case.
- 28.an. Case Prep should automatically gather attachments, reports, narratives, evidence logs, and other relevant materials into a single, exportable package.
- 28.ao. The resulting file should be exportable in ZIP format for submission to prosecutors or other agencies.
- 28.ap. Users should be able to preview and verify contents before finalizing the Case Prep package.
- 28.aq. Case Prep files should be audit-tracked with user, date/time, and version metadata.
- 28.ar. The module should support secure, role-based access to the Case Prep function and allow integration with prosecutor systems for direct digital transfer where applicable.

7. 29. Court Document and Warrant Module for Adults

- 29.a. The proposed RMS should provide a Court Document and Warrant Module for Adults capable of managing the lifecycle of adult court documents and warrants. The module should support the secure creation, tracking, storage, execution, and the archiving of all warrant-related and court-ordered documents.
- 29.b. The module should support creation, review, approval, issuance, and tracking of adult warrant types, including but not limited to:
 - 29.b.1. CJIS Arrest warrants via interface.
 - 29.b.2. Allow linking of adult warrants including but not limited to:
 - 29.b.2a. Individuals: procedutors, defendants, other/additional

29.b.2b. Case report(s)

29.b.2c. Incident(s)

29.b.2d. Arrests

29.b.2e. Charges/offenses

29.b.2f. Evidence

29.b.2g. Link to Master Name Index

29.b.3. Track warrant status, including but not limited to:

29.b.3a. Draft

29.b.3b. Pending approval

29.b.3c. Approved

29.b.3d. Issued

29.b.3e. Served/Executed

29.b.3f. Recalled

29.b.3g. Expired

29.c. Provide automatic notifications to authorized users upon warrant status changes.

29.d. Support attachment of scanned or electronic documents (e.g., affidavits, judicial signatures, court orders).

29.e. Include fields to record, but not limited to:

29.e.1. Issuing authority (judge, court)

29.e.2. Issue date and time

29.e.3. Service instructions

29.e.4. Editable expiration date (if applicable)

29.e.5. Editable expiration period (e.g., 5-year rule)

29.e.6. Notes and comments

29.f. Allow batch import/export and bulk updates of warrant data.

29.g. Allow multiple warrants per individual and case.

29.h. Track officer(s) assigned to serve the warrant.

29.i. Adult Court Document Management should provide the ability to generate, upload, and manage adult

court-related documents, including but not limited to:

- 29.i.1. Subpoenas
- 29.i.2. Summons
- 29.i.3. Court orders
- 29.i.4. Probation/parole conditions

29.j. Allow linking of court documents to:

- 29.j.1. Individuals
- 29.j.2. Case files
- 29.j.3. Officers
- 29.j.4. Court hearings and dates

29.k. Support version control and complete audit history for document edits.

29.l. Provide a repository for standardized adult court document templates.

29.m. Track document service and delivery details:

- 29.m.1. Served by whom, when, and how
- 29.m.2. Proof and affidavit of service
- 29.m.3. Service attempts

29.n. Include automated reminders for upcoming court dates and document deadlines.

29.o. Support electronic signatures and notarization if legally permissible.

29.p. Integration and Interoperability (Adult) should integrate with local, Tennessee, and federal systems, including but not limited to:

- 29.p.1. TBI Warrant Repository Systems
- 29.p.2. National Crime Information Center (NCIC)
- 29.p.3. Court Case Management Systems (CJIS)

29.q. Allow configurable workflows and business rules for adult warrant and document routing and approvals.

29.r. Link to Master Name Index and Personnel / Master Employee Index

29.s. Security and Access Control (Adult) should ensure compliance with CJIS and other applicable security standards and include full audit logging of all user interactions.

29.t. Reporting and Analytics (Adult) should provide pre-built and ad hoc reports, including but not limited to:

29.t.1. Active vs. served warrants

29.t.2.Warrant aging

29.t.3.Court document service rates

29.u. Support export in PDF, XML, Excel, and CSV formats.

29.v. Provide dashboards and visualizations for command staff.

29.w. Provide mobile access for officers to:

29.w.1. Search active adult warrants

29.w.2. View case details

29.w.3. Receive alerts

29.w.4. Update service attempts and status

29.w.5.Support offline access with later synchronization.

30. Juvenile Contact Module

30.a. The RMS shall provide a Juvenile Court Document and Warrant Management Module that is fully segregated from adult data and designed to meet all juvenile justice confidentiality and legal requirements. The module shall support the secure creation, tracking, storage, execution, sealing, and the archiving of juvenile court documents and warrants.

30.b. Juvenile Warrant Management should support creation, review, approval, issuance, and tracking of juvenile warrant types, including but not limited to:

30.b.1. CJIS Juvenile detention warrants

30.b.2. Allow linking of juvenile warrants including but not limited to:

30.b.2a. Individuals: prosecutors, defendants, other/additional

30.b.2b. Case report(s)

30.b.2c. Incident(s)

30.b.2d. Arrests

30.b.2e. Charges/offenses

30.b.2f. Evidence

30.b.2g. Link to Master Name Index and Personnel / Master Employee Index

30.b.2h. Juvenile (May become an Adult at time of arrest.)

30.b.3. Clearly distinguish juvenile records from adult records, enforcing restricted access at all times.

30.b.4. Track warrant status, including but not limited to:

- 30.b.4a. Draft
- 30.b.4b. Pending approval
- 30.b.4c. Approved
- 30.b.4d. Issued
- 30.b.4e. Served/Executed
- 30.b.4f. Recalled
- 30.b.4g. Expired

30.b.5. Provide automated notifications limited to authorized juvenile users.

30.b.6. Support attachment of juvenile-specific documentation (court orders, affidavits, judicial authorizations).

30.b.7. Include fields to record, but not limited to:

- 30.b.7a. Issuing authority (judge, court)
- 30.b.7b. Issue date and time
- 30.b.7c. Service instructions
- 30.b.7d. Editable expiration date (if applicable)
- 30.b.7e. Editable expiration period (e.g., 5-year rule)
- 30.b.7f. Notes and comments

30.b.8. Allow multiple juvenile warrants per individual and case, subject to access restrictions.

30.b.9. Track officer(s) authorized to serve juvenile warrants.

30.b.10. Juvenile Court Document Management should provide the ability to generate, upload, and manage juvenile court-related documents, including but not limited to:

- 30.b.10a. Juvenile custody orders
- 30.b.10b. Detention orders
- 30.b.10c. Juvenile court summons
- 30.b.10d. Court orders specific to juvenile proceedings

30.b.11. Allow linking of documents including but not limited to:

- 30.b.11a. Juvenile individuals

- 30.b.11b. Juvenile case files
- 30.b.11c. Officers
- 30.b.11d. Court hearings and date
- 30.b.11e. Service attempts
- 30.b.11f. Status Offenses
- 30.b.12. Support version control and audit history while preserving confidentiality.
- 30.b.13. Maintain a separate repository for juvenile court document templates.
- 30.b.14. Track document service details, including proof of service, with restricted visibility.
- 30.b.15. Provide alerts for juvenile court dates and statutory deadlines.
- 30.b.16. Support electronic signatures and notarization where legally permitted.
- 30.b.17. Integrate and interoperate with juvenile court and justice systems as authorized by law, including:
 - 30.b.17a. Juvenile Court Case Management Systems
 - 30.b.17b. Approved TBI and federal juvenile justice systems
 - 30.b.17c. Support secure, role-restricted data exchange via APIs.
 - 30.b.17d. Allow configurable juvenile-specific workflows and approval rules.
- 30.b.18. The module should have necessary security and access control, including but not limited to:
 - 30.b.18a. Enforce CJIS, HIPAA (where applicable), and juvenile justice confidentiality statutes.
 - 30.b.18b. Implement enhanced RBAC for juvenile records, including case-based and need-to-know access.
 - 30.b.18c. Maintain comprehensive audit logging for all juvenile record access and changes.
- 30.b.19. Provide juvenile-specific reporting and analytics tools, including but not limited to:
 - 30.b.19a. Juvenile warrant statistics
 - 30.b.19b. Detention and service trends
 - 30.b.19c. Allow exports only to authorized formats and users.
 - 30.b.19d. Support restricted dashboards for authorized supervisory staff.
- 30.b.20. Provide secure mobile access for authorized personnel to:

30.b.20a. View assigned juvenile warrants

30.b.20b. Receive alerts

30.b.20c. Update service attempts

30.b.20d. Enforce additional authentication and offline safeguards.

30.b.21. Comply with all applicable juvenile justice mandates, including but not limited to:

30.b.21a. Strict separation of juvenile and adult data

30.b.21b. Confidentiality and restricted access

30.b.21c. Expungement, sealing, and automatic purging

30.b.21d. Ensure retention schedules are configurable and compliant with local and TN law.

8. **31. Crime Analytics Module**

31.a. The proposed RMS should include an integrated Crime Analytics Module to support real-time and historical analysis of crime data, trends, and patterns. This module should allow analysts, MNPd command staff, and other authorized personnel to effectively evaluate crime data to inform patrol strategies, investigations, community engagement, and resource deployment.

31.b. The Crime Analytics Module should provide tools to analyze, visualize, and report on crime data collected within the RMS.

31.c. The Crime Analytics Module should support ad hoc and scheduled queries and analysis across all relevant data sets, including, but not limited to:

31.c.1. Incident reports

31.c.2. Arrests

31.c.3. Citations

31.c.4. Field interviews

31.c.5. Calls for service (via CAD integration)

31.c.6. Crime classifications and NIBRS/TIBRS and UCR codes

31.d. The module should allow identification and analysis of:

31.d.1. Crime trends over time

31.d.2. Repeat locations

31.d.3. Repeat offenders, victims, or vehicles

31.d.4. Crime series or patterns (e.g., MO, time of day, day of week)

31.d.5. Geographic clustering or mapping of crime incidents

31.e. Support "near-repeat" and temporal analysis (e.g., crimes occurring within a short time/distance interval).

31.f. The module should fully integrate with core RMS modules including, but not limited to:

31.f.1. Incident and Case Reports

31.f.2. Arrests and Bookings

31.f.3. Property and Evidence

31.f.4. Field Interview Reports

31.f.5. CAD data (via Dispatch Integration Module)

31.f.6. Support access to master indexes (names, vehicles, addresses, locations).

31.f.7. Support importing and incorporating data from external systems (e.g., internal databases, regional crime databases, NCIC hits, public crime tip portals).

31.f.7a. Ability to interface with historical MNPd data.

31.f.8. Allow analysts to access structured data via a query builder or SQL-like interface.

31.g. The module should provide advanced search capabilities for filtering data by:

31.g.1. Date/time range

31.g.2. Crime type or classification

31.g.3. Location Type

31.g.4. Geographic area (reporting areas (RPA), zone, radius, or custom polygon)

31.g.5. Suspect/victim demographics

31.g.6. Modus Operandi (MO)

31.g.7. Officer, unit, or reporting area

31.g.8. Support use of Boolean operators and conditional logic in queries.

31.g.9. Allow saving and reusing query templates.

31.g.10. SQL or no-code/low-code query tools for custom reporting.

31.g.11. Ability to filter by incident type, date range, geography, demographics, officer activity, etc.

31.h. The module should include integrated GIS functionality to:

31.h.1. Map incidents, arrests, and other events

31.h.2. Perform hotspot analysis and density mapping

- 31.h.3. Create buffer zones and measure distances
- 31.h.4. Draw and save custom geographic filters (precincts, districts, zones)
- 31.h.5. Display time-based mapping (e.g., animations of crime movement or growth)
- 31.h.6. Integrate with MNPd GIS data or third-party providers (e.g., Esri, Google Maps, ArcGIS)
- 31.i. The module should generate a wide range of reports including, but not limited to:
 - 31.i.1. Crime trends by type, time, location, and demographics
 - 31.i.2. Group A and Group B NIBRS offense codes
 - 31.i.3. Clearance rates and arrest trends
 - 31.i.4. Repeat offender and location reports
 - 31.i.5. Patrol productivity and workload heatmaps
 - 31.i.6. Provide dashboards with:
 - 31.i.6a. Interactive charts (bar, pie, line, stacked)
 - 31.i.6b. Tables with drill-down capabilities
 - 31.i.6c. Key performance indicators (KPIs)
 - 31.i.6d. Configurable views options for different user roles (e.g., MNPd command staff, MNPd Analysts)
 - 31.i.6e. Support scheduled report generation and automated email distribution.
 - 31.i.6f. Export reports to Excel, PDF, CSV, or shareable web links.
 - 31.i.7. Monthly/quarterly/annual crime statistics
 - 31.i.8. Arrest and clearance rates
 - 31.i.9. Incident and call volume trends
 - 31.i.10. Precision Policing crime analysis
 - 31.i.11. Officer performance analytics
 - 31.i.12. Use-of-force trends and compliance analysis
 - 31.i.13. Tactical reports (e.g., shift reports, BOLOs)
 - 31.i.14. Strategic reports (e.g., trend analysis over years)
 - 31.i.15. Administrative reports (e.g., workload distribution, budget justification)
 - 31.i.16. Export options including, but not limited to: PDF, Excel, CSV, XML, JSON.

- 31.i.17. Automated generation of reports
- 31.i.18. Printer-friendly templates for formal reporting.
- 31.i.19. Interactive dashboards for real-time monitoring.
- 31.j. The module should provide link analysis tools to identify connections between, but not limited to:
 - 31.j.1. People
 - 31.j.2. Addresses
 - 31.j.3. Vehicles
 - 31.j.4. Incidents
 - 31.j.5. Property or weapons
 - 31.j.6. Display relationships graphically (e.g., nodes and edges)
 - 31.j.7. Allow filtering based on strength or type of relationship
 - 31.j.8. Support investigation of potential crime series and offender profiles
- 31.k. The module should allow configuration of automatic alerts based on criteria such as:
 - 31.k.1. Spike in crime types or volume
 - 31.k.2. Identification of a suspect matching criteria across incidents
 - 31.k.3. Notify analysts, investigators, or MNPD command staff via in-system alerts or email
- 31.l. Allow sharing of analytical reports and dashboards internally across authorized users.
- 31.m. Provide role-based permissions for viewing, editing, and distributing analysis.
- 31.n. Allow the exporting of crime data and analytics to regional or federal reporting tools (e.g., CompStat).
- 31.o. Enforce role-based access to sensitive crime data and analytical tools.
- 31.p. Allow restricted access to certain queries or datasets based on security clearance or assignment.
- 31.q. Maintain audit logs of all user actions within the Crime Analytics Module.
- 31.r. Web-based or hybrid interface accessible via secure desktop and mobile environments.
- 31.s. Responsive and intuitive user interface for non-technical and technical users alike.
- 31.t. Capable of processing and analyzing large volumes of data with minimal performance degradation.
- 31.u. Allow configuration of default query parameters, dashboards, and KPIs per user or role.
- 31.v. Include tools for data cleanup, normalization, and de-duplication (especially for address and name data).

31.w. The module should have audit trails.

31.x. Module maintains audit logs for all reporting activity.

31.y. MNPd personnel should have the ability to:

31.y.1. Generate standardized and ad hoc reports through an intuitive, query-based interface

31.y.2. Create and save custom report templates that align with MNPd's operational and analytical needs.

9. **32. Dispatch/CAD Integration Module**

32.a. The proposed RMS should include a fully integrated Dispatch/CAD Integration Module that enables seamless, real-time data exchange between the RMS and Davidson County DEC's Motorola Computer-Aided Dispatch (CAD) system. The integration should support retrieval of incident data, minimizing duplicate data entry, enhancing officer safety, and streamlining case management workflows.

32.b. Additionally, the module must support receiving Next Generation 911 (NG911) advanced 911 call data, including multimedia content and enhanced caller location is available within the RMS for situational awareness, investigation, and long-term case management.

32.c. The Dispatch/CAD Integration Module should automatically import CAD incident data into the RMS in real-time or near-real-time, including, but not limited to:

32.c.1. CAD event number

32.c.2. MNPd Incident number

32.c.3. Date and time of call receipt, dispatch, arrival, and clearance

32.c.4. Dispatch narrative and notes

32.c.5. Call type/nature (10-Codes and Phonetic Alphabet)

32.c.6. Location details (mapped and textual)

32.c.7. Caller information (name, phone number, relationship to incident)

32.c.8. Involved persons, vehicles, and property (if available)

32.c.9. Officer(s) and unit(s) assigned

32.c.10. Disposition or final call outcome

32.d. The module should support NG911 multimedia elements, such as:

32.d.1. Audio recordings (e.g., emergency calls)

32.d.2. Text-to-911 messages

32.d.3. Images or videos submitted by callers or transferred from Public Safety Answering Points (PSAPs)

32.e. The module should allow RMS users to search and retrieve CAD call history by:

32.e.1. CAD event number

32.e.2. Incident number

32.e.3. Date/time range

32.e.4. Address/location

32.e.5. Officer/unit

32.e.6. Incident type

32.f. Enable auto-population of RMS incident reports using CAD and NG911 data to reduce redundant data entry.

32.g. The integration for this module should:

32.g.1. Support real-time or near-real-time receive only data exchange.

32.g.2. Be compatible with third-party CAD systems via:

32.g.2a. Web services (REST or SOAP APIs)

32.g.2b. Motorola CAD, listed in the MNPd RMS Interfaces section.

32.g.3. Standard data formats such as XML, JSON, or NIEM-compliant structures

32.g.4. Be NG911-capable, supporting integration with Emergency Services IP Networks (ESInet) and NGCS (Next Generation Core Services) components.

32.g.5. Support linking of NG911-compliant multimedia files and metadata, linking them to relevant CAD and RMS records, upon request.

32.g.6. Ability to accommodate a variety of CAD vendors and versions, including proprietary and open-source systems.

32.g.7. Allow configurable field mappings between CAD and RMS data elements.

32.g.8. Support asynchronous and fail-safe message processing to ensure reliability and data integrity.

32.g.9. Maintain persistent linking between RMS incident and case numbers and originating CAD event numbers.

32.h. RMS incident creation should be initiated automatically or manually from CAD events.

32.i. Support consolidation of multiple CAD calls into a single RMS case (e.g., multiple calls for the same incident).

32.j. Allow the linking of NG911 multimedia (e.g., caller-submitted photos, videos, or chat transcripts) to RMS records when provided by the CAD.

32.k. Maintain a clear status for imported CAD events (e.g., "Imported," "Report Pending,").

- 32.l. Display officer status and unit location information in RMS (if supported by CAD).
- 32.m. Provide a full audit trail of data received from CAD, including, but not limited to:
 - 32.m.1. Timestamps of import/update
 - 32.m.2. User(s) modifying linked records
 - 32.m.3. Any rejected or failed transmissions
 - 32.m.4. Log all integration-related errors and generate alerts for system administrators.
 - 32.m.5. Log access to NG911 multimedia content separately to ensure privacy and chain-of custody tracking.
- 32.n. The module should enable search of CAD-linked events within RMS by:
 - 32.n.1. CAD event number or RMS incident number
 - 32.n.2. Address or location
 - 32.n.3. Involved parties officers
 - 32.n.4. Call type or disposition
 - 32.n.5. Display linked CAD and NG911 data inline within RMS reports for full situational context.
- 32.o. The module should support reporting on:
 - 32.o.1. RMS incidents initiated from CAD vs. manually entered.
 - 32.o.2. Time from CAD event creation to RMS report submission.
 - 32.o.3. Officer or unit workload (based on CAD events).
 - 32.o.4. Volume and type of NG911 call content (text, image, video) associated with cases.
- 32.p. Include dashboards and summary views of CAD-to-RMS activity volume and status.
- 32.q. Support both cloud-hosted and on-premises data storage models.
- 32.r. Ensure secure data transmission between CAD, RMS and NG911-enabled sources using encryption.
- 32.s. Support high availability and failover mechanisms for continuous data exchange.
- 32.t. Provide APIs or SDKs for integration with custom or legacy CAD and NG911 systems.
- 32.u. Enforce role-based access to CAD-linked and NG911-originated information in the RMS.
- 32.v. Mask or redact sensitive CAD data (e.g., juvenile names, victim information) based on user roles or permissions.
- 32.w. Comply with NENA i3 and other applicable security standards.
- 32.x. Provide tools for administrators to:

32.x.1. Monitor CAD-RMS integration status

32.x.2. Update data mapping rules as needed

32.y. Offeror will support integration troubleshooting, including, but not limited to:

32.y.1. Error resolution

32.y.2. Log review

32.z. Compatibility updates after CAD, RMS, and NG911 upgrades

33. Field Contact Module

33.a. The proposed RMS should include a fully integrated Field Interview (FI) Reports Module to enable law enforcement personnel to document, manage, and analyze non-custodial contacts with subjects in the field. The module should support mobile and in-office data entry and ensure that all data is searchable, reportable, and securely stored in compliance with applicable laws and departmental policies.

33.b. The module should allow officers to create, edit, and submit FI reports both in the field and from office workstations.

33.c. The module should Capture comprehensive field interview data including, but not limited to:

33.c.1. Date and time of contact

33.c.2. Location (with mapping/GPS integration if possible)

33.c.3. Subject(s) information (name, DOB, race, sex, address, identifiers)

33.c.4. Officer(s) involved

33.c.5. Reason for contact

33.c.6. Narrative summary of the contact

33.c.7. Observed behaviors or statements made

33.c.8. Associated vehicles, persons, groups or gangs

33.c.9. Photos or other attachments (e.g., scanned ID, tattoos, group/gang insignia)

33.d. Allow documentation of multiple individuals and vehicles per FI report.

33.e. Link Associated Contacts, when possible.

33.f. Include the ability to tag interviews as potentially related to:

33.f.1. Group/Gang activity

33.f.2. Narcotics

33.f.3. Known criminal offenders

33.f.4. Suspicious behavior

33.f.5. Terry Stop

33.g. The module should seamlessly integrate with:

33.g.1. CAD for importing contact details

33.g.2. Mobile systems (MDTs, tablets, mobile apps)

33.g.3. Master Name Index, Master Vehicle Index, and Master Location Index

33.g.4. Crime Analysis tools for pattern recognition and link analysis

33.g.5. Gang Intelligence and Criminal Intelligence modules

33.h. Allow field interview reports to be associated with:

33.h.1. Related incidents, cases, arrests, citations, and BOLOs

33.h.2. Enable synchronization with agency intelligence databases and regional information sharing systems (e.g., regional RMS, fusion centers, Regional Information Sharing Systems (RISS)).

33.i. Provide robust search capabilities based on:

33.i.1. Person name/DOB/physical descriptors

33.i.2. Location (with radius or map-based search)

33.i.3. Officer ID or unit

33.i.4. Time/date range

33.i.5. Keywords from narratives

33.i.6. Gang or group affiliation

33.j. Allow users to filter by FI report status (e.g., submitted, reviewed, flagged).

33.k. Support link analysis tools to visualize associations between subjects, vehicles, and locations.

33.l. The module should have a configurable workflow for:

33.l.1. Officer submission

33.l.2. Optional MNPd command staff review

33.l.3. Allow returned reports for corrections with tracking of revisions

33.l.4. Status tracking (e.g., draft, pending, approved, archived)

33.m. Automatic alerts for:

- 33.m.1. Repeat contacts with individuals of interest
- 33.m.2. Matches to BOLOs, warrants, or known offenders
- 33.m.3. Potential gang affiliations or known criminal patterns
- 33.m.4. Ability to flag FIs for further review or intelligence follow-up
- 33.n. Generate standard and ad hoc reports such as:
 - 33.n.1. Field interviews by officer, location, or shift
 - 33.n.2. Contacts with persons flagged as gang-affiliated
 - 33.n.3. Repeat field interviews of the same individual
 - 33.n.4. Trends by location, time of day, or crime type
 - 33.n.5. Export report formatting including, but not limited to: PDF, Excel, CSV
 - 33.n.6. Support dashboards with visualizations (charts, heat maps, etc.)
- 33.o. Enforce role-based access to:
 - 33.o.1. View, create, or edit FI reports
 - 33.o.2. Access sensitive intelligence-related information
 - 33.o.3. Audit log of all changes to FI reports
 - 33.o.4. Ability to restrict visibility of reports based on sensitivity (e.g., open intelligence cases, juvenile contacts)
 - 33.o.5. Compliance with CJIS and 28 CFR Part 23 (where applicable)
- 33.p. User Interface (UI) optimized for both desktop and mobile use
- 33.q. Touchscreen-compatible entry forms with dropdowns, auto-fill fields, and code lists
- 33.r. Allow for quick entry via voice-to-text or keyboard shortcuts
- 33.s. Print-friendly view and mobile-friendly formats
- 33.t. Support for photo capture and attachment via mobile devices
- 33.u. Allow configuration of data retention policies based on MNPD requirements
- 33.v. Support the archiving of inactive or outdated FI reports
- 33.w. Allow flagging of FI reports for long-term retention due to intelligence value.
- 33.x. Support free-text narratives with spell check and formatting tools.
- 33.y. Utilize a point system of questions to establish if person may be in a gang.

10. **34. Fugitives Module**

34.a. The proposed RMS should include a fully integrated Fugitives Module that allows agencies to document, track, prioritize, and manage individuals classified as fugitives from justice. This includes individuals with active warrants, extraditable charges, or who have absconded supervision. The module should support investigative workflows, NCIC integration, officer safety notifications, and analytics related to fugitive apprehension.

34.b. The Fugitives Module should integrate with the Master Person Index, Master Location Index, Master Vehicle Index, Warrants, BOLOs, Arrests, Cases, and Field Interview modules.

34.c. Module should allow the creation and management of fugitive records, linking them to warrant data, case files, and investigative notes.

34.d. Each fugitive record should have a unique identifier and be linked to the associated individual's person record.

34.e. Module should support classification of fugitives by type, priority level, and MNPD defined risk assessments.

34.f. The module should support the following classifications (at minimum):

34.f.1. Violent offender

34.f.2. Sex offender

34.f.3. Extraditable fugitive

34.f.4. Federal /TN/local jurisdictional authority

34.f.5. Supervision absconder (e.g., parole, probation)

34.g. Module should allow agencies to define custom risk levels (e.g., Low, Medium, High, Critical) and assign color-coded flags.

34.h. Module should allow assignment of fugitives to specialized units (e.g., MNPD personnel supporting the US Marshall's Task Force and the FBI Task Force).

34.i. Priority status should support sorting, filtering, and alerting functions within the RMS.

34.j. Each fugitive record should support detailed information, including, but not limited to:

34.j.1. Full name, aliases, nicknames

34.j.2. Date of birth, SSN, physical descriptors

34.j.3. Photographs, mugshots, identifying marks

34.j.4. Last known address, employer, associates

34.j.5. Associated warrant information (number, issuing agency, charges, bond amount)

34.j.6. Extradition limitations (e.g., region, state, nationwide)

34.j.7. Known weapons, violent history, or mental health concerns

- 34.j.8. Flight risk indicators or history of evasion
- 34.k. Module should support the attachment of documents, images, reports, surveillance photos, and intelligence memos.
- 34.l. Module should track contacts, sightings, field interviews, tips, and investigative notes chronologically.
- 34.m. Module should support linkage to NCIC and/or TBI warrant databases for real-time warrant validation and status updates.
- 34.n. Module should allow automated flagging of fugitives with active NCIC warrants.
- 34.o. NCIC-required data fields should be supported, with built-in data validation to ensure compliance prior to submission.
- 34.p. Module should support automated or manual updates to warrant status (e.g., cleared, recalled, served, service attempts).
- 34.q. Module should support tracking of leads, sightings, field interviews, and contacts associated with the fugitive.
- 34.r. Investigators should be able to assign tasks or investigative steps to specific personnel.
- 34.s. Module should provide officer safety alerts during queries or encounters with individuals flagged as fugitives.
- 34.t. Alerts should include violent tendencies, known associates, weapons history, or other relevant safety considerations.
- 34.u. Module should allow automated generation of BOLOs and link fugitive records directly to them.
- 34.v. Module should allow recording incarceration state, if available.
- 34.w. The module should support advanced search of fugitive records by:
- 34.w.1. Name, alias, DOB, physical descriptors
 - 34.w.2. Warrant type or charge severity
 - 34.w.3. Priority level or agency-assigned task force
 - 34.w.4. Last known location or jurisdiction
 - 34.w.5. Warrant status or extradition status
 - 34.w.6. Search results should support drill-down into the full fugitive profile, warrant information, related cases, and contacts.
- 34.x. Module should allow filters by region, squad assignment, risk level, and offense type.
- 34.y. Module should support geolocation tagging of fugitive-related intelligence (e.g., last seen location, known associates).
- 34.z. Module should allow viewing of fugitives on integrated maps, color-coded by risk level or priority.

- 34.aa. The map interface should support layering of incidents, BOLOs, field contacts, or warrant service attempts.
- 34.ab. Users should be able to define geographic search radii and proximity alerts.
- 34.ac. Module should support real-time alerts when a fugitive is encountered in any module (e.g., field interview, arrest, CAD call).
- 34.ad. Alerts should be visible to dispatchers, patrol officers, investigators, and booking personnel as appropriate.
- 34.ae. Module should allow task assignment and notification to fugitive squads or responsible investigators.
- 34.af. Supervisors should be able to configure alert thresholds based on fugitive classification or case urgency.
- 34.ag. The module should support standard and ad hoc reports including, but not limited to:
 - 34.ag.1. Active fugitive list by classification or priority
 - 34.ag.2. Apprehension rates over time
 - 34.ag.3. Fugitives by offense type or jurisdiction
 - 34.ag.4. Task force activity reports
 - 34.ag.5. Module should support export of reports in PDF, Excel, and CSV formats.
 - 34.ag.6. Users should be able to generate dashboards and visualizations (e.g., heat maps, pie charts, time-to-apprehension metrics).
- 34.ah. Access to the Fugitives Module should be role-based and restrict sensitive data to authorized users.
- 34.ai. Module should support tiered access (e.g., patrol vs. investigative units vs. supervisors).
- 34.aj. All access, edits, or views of fugitive records should be logged and auditable.
- 34.ak. Administrators should be able to configure access by unit, assignment, or clearance level.
- 34.al. Administrators should be able to configure:
 - 34.al.1. Fugitive classifications and risk levels
 - 34.al.2. Extradition zones and flags
 - 34.al.3. Custom fields for MNPd specific requirements
 - 34.al.4. Notification templates and scheduling
- 34.am. Module should support data cleanup tools to merge duplicate records and flag inconsistencies.
- 34.an. Users should be able to archive resolved fugitive records while maintaining full historical access.

35. Group/Gang Tracking Module

35.a. The proposed RMS should include a fully integrated Group Tracking Module (also referred to as Gang Tracking Module) that enables the identification, documentation, tracking, and analysis of criminal groups and their members, including street gangs, prison gangs, organized crime groups, and other threat-based organizations. The module should support intelligence gathering, officer safety, reporting, and inter-agency collaboration in compliance with federal and TN standards for criminal intelligence systems.

35.b. Module should provide a dedicated Group Tracking Module integrated with the RMS Master Name Index.

35.c. Module should support the documentation of group names, aliases, types, identifiers, symbols, and territories.

35.d. Module should allow tracking of both confirmed and associate members with appropriate status indicators (e.g., validated, associate, suspected).

35.e. Each group should have a unique identifier, with the ability to associate it with incidents, arrests, field interviews, property, and cases.

35.f. Module should support intelligence-led policing by allowing group affiliations to be factored into risk assessments and case prioritization.

35.g. The module should allow for the creation and management of group profiles, including the following fields:

35.g.1. Group name and aliases

35.g.2. Classification (e.g., street gang, prison gang, extremist group)

35.g.3. Primary activities/criminal enterprises

35.g.4. Known turf or operational area

35.g.5. Known rivals or alliances

35.g.6. Symbols, tattoos, hand signs, colors

35.g.7. Known communication methods or hierarchy

35.h. Group profiles should allow for the attachment of images, documents, videos, or graffiti photos.

35.i. Module should support the linking of groups to other groups (e.g., alliances, rivalries).

35.j. Module should allow flags for officer safety, known violent tendencies, or use of weapons.

35.k. The module should support associating persons with a group and documenting:

35.k.1. Membership status (validated, associate, suspected, former)

35.k.2. Entry date and method (self-admitted, tattoos, witness, law enforcement intelligence)

35.k.3. Rank/role (e.g., leader, enforcer, recruiter)

35.k.4. Affiliated group(s)

35.l. Module should allow multiple validation criteria based on configurable MNPDP policies and applicable legal standards.

- 35.m. Module should capture the basis for validation and provide audit trails for any changes to validation status.
- 35.n. Module should support historical tracking of membership changes over time.
- 35.o. Module should allow visualization of associations between individuals and groups, including link analysis or network mapping.
- 35.p. Users should be able to view relationships such as familial ties, co-arrests, field contacts, phone records, or co-location at incidents.
- 35.q. Module should allow visual overlays showing territories, hotspots, or known activity zones on integrated maps.
- 35.r. Module should allow linking of members and groups to criminal events, intelligence reports, or BOLOs.
- 35.s. Module should allow advanced search across groups, members, locations, identifiers (e.g., tattoos, nicknames), and associations.
- 35.t. Users should be able to filter by group type, activity level, validation status, geographic area, or involvement in specific crimes.
- 35.u. Users should be able to search for persons affiliated with multiple groups or those with high-risk designations (e.g., violent, armed).
- 35.v. Search results should support drill-down into group and individual profiles with all linked records.
- 35.w. Module should alert users when interacting with individuals or locations associated with gangs or criminal groups.
- 35.x. Alerts should display gang affiliation, validation status, violent history, and officer safety notes during person/vehicle queries, incident entry, or arrests.
- 35.y. Users should be able to configure alert levels or flags (e.g., leader, high-risk associate, known to carry weapons).
- 35.z. Module should support analytical reporting on gang activity trends, membership changes, geographic influence, and violent crimes linked to groups.
- 35.aa. Users should be able to generate reports including, but not limited to:
- 35.aa.1. Group membership rosters
 - 35.aa.2. Incident and arrest summaries by group
 - 35.aa.3. Validation history reports
 - 35.aa.4. Territorial activity maps
- 35.ab. Module should support heat mapping and statistical dashboards for MNPd command staff or gang units.
- 35.ac. Module should support the exporting of reports in standard formats (e.g., PDF, CSV, Excel) and automated scheduling for periodic distribution.
- 35.ad. Module should provide strict access controls to the Gang Module based on roles, units, and security clearance.
- 35.ae. Access to gang intelligence should be logged and auditable, including views, edits, and exports.
- 35.af. Module should support marking of sensitive records (e.g., informants, undercover operations) with tiered access levels.

- 35.ag. Module should comply with applicable TN/federal criminal intelligence system standards.
- 35.ah. Module should support secure information sharing with regional or federal gang databases (e.g., Regional Information Sharing Systems (RISS), FBI NGIC), where authorized.
- 35.ai. Module should support integration with other RMS or intelligence platforms for cross jurisdictional group tracking.
- 35.aj. Module should allow user-defined sharing rules and auditing of what intelligence is shared and with whom.
- 35.ak. Module should support federated search and federated identity matching across multiple data sources.
- 35.al. Module should link to Incident, Case Management, Juvenile Contact, Master Name Index, and Field Contact modules.
- 35.am. Administrators should be able to configure group types, membership statuses, validation criteria, and flags without Offeror assistance.
- 35.an. Module should allow for the import/export of group data for interagency coordination.
- 35.ao. Module should provide data cleansing tools to merge duplicate group records or flag inconsistent data.
- 35.ap. Module should support archiving or deactivating disbanded groups while maintaining full historical access.

36. Human Resources/Personnel Module

- 36.a. Module should be seamless with the overall RMS.
- 36.b. All data should comply with applicable federal, TN, and local regulations (e.g., CJIS, HIPAA, FLSA, EEOC).
- 36.c. Role-based access controls should be enforced to protect sensitive personnel data.
- 36.d. Alignment to MNPd's Bureau, Division, Section, Unit, Shift (BDSU/Shift) organizational structure.
- 36.e. Module should maintain a complete audit trail of all changes to personnel records.
- 36.f. Module should support both sworn officers and civilian staff.
- 36.g. Store comprehensive employee profiles, including, but not limited to:
 - 36.g.1. Full name, date of birth, gender at birth, and contact information
 - 36.g.2. Employee ID, badge number, rank/position, division/unit
 - 36.g.3. Employment type (sworn, civilian, contractor)
 - 36.g.4. Date of hire, status (active, suspended, retired, terminated)
 - 36.g.5. Supervisor information
 - 36.g.6. Emergency contact details
- 36.h. Track certifications, licenses, and renewals (e.g., POST certification, firearm qualifications).
- 36.i. Document security clearance levels.

- 36.j. Track issued equipment and uniforms via link to Asset Management Module.
- 36.k. Maintain the history of assignments, transfers, promotions, demotions.
- 36.l. Track all training courses attended, dates, scores, and certification expiration dates.
- 36.m. Allow scheduling and tracking of mandatory and elective training.
- 36.n. Alert users to upcoming or expired certifications and training requirements.
- 36.o. Maintain instructor credentials and course materials.
- 36.p. Track employee evaluations and performance reviews.
- 36.q. Store commendations, awards, and recognition.
- 36.r. Record disciplinary actions, internal investigations, complaints, and outcomes.
- 36.s. Support case linkage to personnel involved for early intervention or performance review (e.g., response to resistance reports, citizen complaints).
- 36.t. Maintain and manage employee schedules.
- 36.u. Track psychological evaluations.
- 36.v. Track physical fitness test results, medical exams.
- 36.w. Monitor compliance with departmental health and wellness policies.
- 36.x. Securely store medical records with access restrictions per HIPAA and CJIS guidelines.
- 36.y. Track applicants, background checks, polygraph results, interview outcomes.
- 36.z. Store hiring documents, offer letters, and onboarding checklists.
- 36.aa. Track probationary period evaluations and status changes.
- 36.ab. Intuitive dashboards for different roles (HR, supervisors, MNPd command staff).
- 36.ac. Document resignation, retirement, termination, or other separation types.
- 36.ad. Track exit interviews, return of equipment, and clearance of outstanding obligations.
- 36.ae. Maintain historical records post-separation with configurable retention policies.
- 36.af. Generate reports on:
 - 36.af.1. Staffing levels and distribution
 - 36.af.2. Certification status and compliance
 - 36.af.3. Training history and gaps
 - 36.af.4. Disciplinary actions and trends
 - 36.af.5. Diversity and inclusion metrics

- 36.af.6. Support ad-hoc reporting and data exports (PDF, XPS, CSV, XML, etc.).
- 36.ag. Provide dashboard views for MNPd command staff.
- 36.ah. The module should Interface with:
 - 36.ah.1. Benchmark Analytics, INC (future consideration)
 - 36.ah.2. Payroll and timekeeping systems (Currently: OCD Oracle Cloud and INFOR Workbrain)
 - 36.ah.3. Internal Affairs systems (Currently: IAPro/BlueTeam)
 - 36.ah.4. Master Employee Index
- 36.ai. Support data import/export via standard APIs (RESTful, JSON, XML).
- 36.aj. Maintain compliance with the CJIS Security Policy for data sharing and access.
- 36.ak. Enforce role-based permissions (e.g., HR staff, supervisors, auditors).
- 36.al. Log all access and changes to personnel records.
- 36.am. Support data retention and purging policies based on legal requirements.
- 36.an. Provide audit logs for internal and external reviews.

37. Impound Management Module

- 37.a. The RMS should allow authorized personnel to create, and update impound records.
- 37.b. Each impound record should include:
 - 37.b.1. Unique Impound Record ID (auto-generated)
 - 37.b.2. Date and time of impound
 - 37.b.3. Impounding officer's name, badge/ID number
 - 37.b.4. Reason for impound (e.g., evidence, abandoned, traffic violation, stolen recovery)
 - 37.b.5. Impound location (geolocation optional)
 - 37.b.6. Tow company and contact details
 - 37.b.7. Associated incident number(s)
 - 37.b.8. Chain of custody tracking
- 37.c. For vehicles, the RMS should capture:
 - 37.c.1. Make, model, year, color
 - 37.c.2. VIN
 - 37.c.3. License plate number and state

- 37.c.4. Registration expiration
- 37.c.5. Odometer reading (if available)
- 37.c.6. Condition at time of impound (with optional image attachments)
- 37.d. For non-vehicle property, the RMS should allow:
 - 37.d.1. Description of item(s)
 - 37.d.2. Quantity
 - 37.d.3. Identifying marks or serial numbers
 - 37.d.4. Classification (e.g., evidence, found property, hazardous)
- 37.e. The RMS should record:
 - 37.e.1. Owner's name, address, and contact information (if known)
 - 37.e.2. Driver/possessor at time of impound (if different from owner)
 - 37.e.3. Associated citations, arrests, or case numbers
- 37.f. The RMS should track:
 - 37.f.1. Tow request details (date/time, requested by, method)
 - 37.f.2. Tow truck operator/company
 - 37.f.3. Tow authorization details (officer name, signed forms, etc.)
- 37.g. Storage location (MNPd impound lot, evidence garage, other third-party facility)
- 37.h. Lot or space number (if applicable)
- 37.i. Towing and storage fees (optional financial tracking)
- 37.j. Hold type and status (e.g., no hold, evidence hold, pending release)
- 37.k. Miscellaneous non-vehicles that are stored at the Impound Lot
- 37.l. The module should support:
 - 37.l.1. Entry and removal of administrative or investigative holds
 - 37.l.2. Reason for hold and authorizing party
 - 37.l.3. Documentation for release (e.g., proof of ownership, court order, payment of fees)
 - 37.l.4. Release date/time, recipient information, and releasing officer
 - 37.l.5. Digital signature or acknowledgment of release
 - 37.l.6. Audit trail of hold/release actions

37.m. The module should link impounded items to:

- 37.m.1. Associated cases, evidence records, and reports
- 37.m.2. Property room or evidence module (if applicable)
- 37.m.3. Investigating officer(s) or units
- 37.m.4. Incident number

37.n. The module should track:

- 37.n.1. Final disposition (e.g., returned to owner, auctioned, destroyed, forfeited)
- 37.n.2. Date and method of disposal
- 37.n.3. Authorizing documentation or court orders
- 37.n.4. Third-party auction or disposal Offeror information
- 37.n.5. Fees collected or waived (optional)

37.o. The module should support:

- 37.o.1. Automated alerts for approaching legal retention deadlines
- 37.o.2. Hold expiration or release eligibility
- 37.o.3. Notifications to impound administrators, investigators, or property owners (if configured)

37.p. The module should allow uploading of:

- 37.p.1. Photos of the vehicle/property at time of impound
- 37.p.2. Impound authorization forms
- 37.p.3. Towing receipts, court orders, or other legal documents

37.q. The module should support advanced search and filtering by date, officer, vehicle details, case number, owner name, hold status

37.r. The module should generate reports including, but not limited to:

- 37.r.1. Daily/weekly/monthly impound logs
- 37.r.2. Inventory of items currently in impound
- 37.r.3. Vehicles pending release or disposal
- 37.r.4. Audit logs of impound activity
- 37.r.5. Chain of custody reports

37.s. The module should enforce:

- 37.s.1. Audit logging of all changes, with timestamps and user IDs

37.s.2. Restricted access to evidence or hold information where necessary

37.t. The module should support integration with:

37.t.1. CAD and Incident Reporting modules

37.t.2. Evidence and Property Management modules

37.t.3. Vehicle Registration databases (DMV/MVD lookup)

37.t.4. Third-party towing and storage systems (optional)

11. **38. Incident Management Module**

38.a. The Incident Module shall serve as a core component of the RMS and integrate seamlessly with all other RMS modules.

38.b. The module should facilitate standardized data collection, comply with all applicable national and TN-level reporting mandates (e.g., NIBRS/TIBRS, LEOKA) and ensure timely information sharing among authorized users and agencies.

38.c. Ability to initiate an incident report directly from CAD, or manually through the RMS.

38.d Capture and classify incident types using agency-defined codes and standardized classifications (e.g., NIBRS/TIBRS offense codes).

38.e. Support multiple offenses and persons involved within a single incident.

38.f. Ability to provide unique incident numbers, with a configurable numbering schema based on MNPd needs.

38.g. Allow entry of free-text narratives with formatting tools (bold, underline, spellcheck).

38.h. Allow for Copy and Paste capability.

38.i. Support template-driven report structures for different incident types.

38.j. Enable officers and supervisors to append supplemental reports.

38.k. Automatically log all narrative edits, additions, and deletions with date/time/user stamps.

38.l. Record detailed information on all persons involved in an incident (e.g., suspects, victims, witnesses, reporting parties, injury details).

38.m. Interface with the Master Name Index (MNI) to pull or add individual records.

38.n. Allow tracking of relationships between involved parties.

38.o. Capture photos, physical descriptors, contact details, aliases, and identification numbers.

38.p. Allow for the recording of individuals with incomplete data into a separate table including field for Person Type (e.g., Suspect, Victim, Witness).

38.q. Associate stolen, recovered, or damaged property with an incident.

38.r. Interface with the Property and Evidence Module to enable chain-of-custody tracking.

- 38.s. Include fields for; make, model, serial number, value, status, and recovery details.
- 38.t. Record vehicle data including year, make, model, VIN, license plate, and status (e.g., stolen, recovered).
- 38.u. Interface with the Master Vehicle Index and state motor vehicle databases.
- 38.v. Allow for the recording of vehicles with incomplete data into a separate table.
- 38.w. Allow for incomplete information for searches.
- 38.x. Allow ability to force location.
- 38.y. Provide configurable multi-level report approval processes (e.g., officer to supervisor to records division).
- 38.z. Allow reviewers to provide comments and return reports for corrections. Provide audit trails for approval actions.
- 38.aa. Allow attachment of photos, videos, PDFs and audio recordings to incident reports.
- 38.ab. Store all attachments securely and associate them with appropriate incident numbers.
- 38.ac. Support viewing from mobile and desktop devices.
- 38.ad. Enable linkage between, but not limited to incidents, arrests, cases, persons, vehicles, and property.
- 38.ae. Provide incident merge and split functionality with audit trails.
- 38.af. Present cross-referenced data in a user-friendly, visual manner (e.g., link analysis diagrams).
- 38.ag. Support advanced search by incident number, date range, location, party involved, offense type, or keyword.
- 38.ah. Ability to add custom fields.
- 38.ai. Generate standard and custom reports for supervisory and statistical review.
- 38.aj. Export reports in multiple formats (PDF, Excel, CSV).
- 38.ak. Remain compliant with current FBI NIBRS/TIBRS reporting requirements.
- 38.al. Allow for incident submission to TN crime reporting repositories.
- 38.am. Provide error checking and validation for NIBRS/TIBRS compliance prior to submission.
- 38.an. Display incident locations on an interactive GIS map.
- 38.ao. Allow spatial analysis (e.g., heat maps, clustering).
- 38.ap. Enable geographic filtering in searches and reporting.
- 38.aq. Allow advanced text input searches for any field.

38.ar. Full audit logging of all access and changes to incident records.

38.as. Support for CJIS compliance and multi-factor authentication.

38.at. Interface with external systems such as CAD, DCSO Jail Management System, Davidson County Court Systems, and external data repositories via standard protocols (e.g., REST API, XML, NIEM).

38.au. Support data exchange with NCIC and TIBRS.

38.av. Allow mobile users (e.g., in patrol vehicles) to initiate and complete incident reports.

38.aw. Sync data automatically when connectivity is restored if operating offline.

39. Master Indices Modules

39.a. The proposed Records Management System (RMS) shall provide five (5) centralized Master Indices modules to maintain authoritative records for persons, vehicles, locations, property, and organizations encountered during law enforcement operations. These index modules shall serve as enterprise-wide repositories that support incident reporting, investigations, intelligence gathering, field operations, records management, data quality, and information sharing. The solution shall provide comprehensive Master Index functionality including record creation, maintenance, deconfliction, search, linkage analysis, auditing, security controls, and integration with internal and external systems.

39.b. General Requirements Applicable to the Master Indices which include Master Name Index Module, Master Vehicle Index Module, Master Location Index Module, Master Property Index Module, and Master Organization Index Module as further detailed below.

39.b.1. The RMS shall have the following data management:

39.b.1a. Maintain a single authoritative master record for each indexed entity.

39.b.1b. Automatically identify potential duplicate records.

39.b.1c. Provide configurable merge, split, and deconfliction processes.

39.b.1d. Ability to provide rollback or recovery options to undo any merge, split or deconfliction process.

39.b.1e. Maintain historical and inactive records without data loss.

39.b.1f. Support unlimited cross-references between indexed entities.

39.b.1g. Allow user-defined aliases, alternate identifiers, and supplemental information.

39.b.1h. Support configurable validation rules and business logic.

39.b.1i. Track source system and originating agency information.

39.b.1j. Maintain complete audit trails of all additions, modifications, merges, and deletions.

39.b.2. The RMS shall have the following search and retrieval:

39.b.2a. Provide enterprise-wide searching across all master indices.

- 39.b.2b. Support exact, partial, phonetic, fuzzy, wildcard, and proximity searches.
- 39.b.2c. Support advanced filtering and query criteria.
- 39.b.2e. Display search results in configurable formats.
- 39.b.2f. Provide rapid response times for large datasets.
- 39.b.2g. Support saved searches and query templates.
- 39.b.3. The RMS shall have the following relationship management:
 - 39.b.3a. Allow users to establish and maintain relationships among persons, vehicles, locations, property, organizations, incidents, arrests, citations, warrants, and cases.
 - 39.b.3b. Display graphical relationship views.
 - 39.b.3c. Support one-to-one, one-to-many, and many-to-many relationships.
 - 39.b.3d. Provide timeline and association tracking capabilities.
- 39.b.4. The RMS shall the following security:
 - 39.b.4a. Enforce role-based access controls.
 - 39.b.4b. Support field-level security and redaction.
 - 39.b.4c. Restrict access based upon user role, assignment, bureau, unit, or security classification for both MNPd internal use and external agencies.
 - 39.b.4d. Maintain CJIS-compliant auditing and security controls.
 - 39.b.4e. Log all record access, modifications, exports, and prints.
- 39.b.5. The RMS shall have the following integration:
 - 39.b.5a. Integrate with CAD, JMS, evidence systems, citation systems, state repositories, NCIC interfaces, NIBRS/TIBRS reporting, and external justice systems.
 - 39.b.5b. Support API-based integrations.
 - 39.b.5c. Allow external systems to query and update master index records through controlled interfaces.
- 39.b.6. The RMS shall provide reporting and analytics capabilities across all Master Indices, including, but not limited to:
 - 39.b.6a. Entity relationship analysis.
 - 39.b.6b. Link analysis visualization.
 - 39.b.6c. Pattern and trend identification.
 - 39.b.6d. Repeat offender analysis.

- 39.b.6e. Repeat location analysis.
- 39.b.6f. Vehicle association analysis.
- 39.b.6g. Property recovery analysis.
- 39.b.6h. Organization affiliation analysis.
- 39.b.6i. Intelligence and investigative reporting.
- 39.b.6j. User-configurable dashboards and reports.
- 39.b.6k. Export capabilities to common formats.
- 39.b.6l. Ad hoc query and reporting tools.

39.c. The RMS Must contain at a minimum the five major indices listed below.

39.d. The Master Name Index Module shall maintain a centralized repository of all persons encountered by the agency and do the following:

- 39.d.1. Create and maintain a unique master name record.
- 39.d.2. Store multiple names including:
 - 39.d.2a. Full legal names
 - 39.d.2b. Aliases
 - 39.d.2c. Nicknames
 - 39.d.2d. Maiden names
 - 39.d.2e. Previous names
 - 39.d.2f. Gang monikers
- 39.d.3. Capture personal information including but not limited to:
 - 39.d.3a. Date of birth
 - 39.d.3b. Gender
 - 39.d.3c. Race
 - 39.d.3d. Ethnicity
 - 39.d.3e. Height
 - 39.d.3f. Weight
 - 39.d.3g. Eye color
 - 39.d.3h. Hair color

39.d.3i. Physical descriptors

39.d.3i.1. Scars, marks, tattoos

39.d.3i.2. Mugshots/biometric photos

39.d.3i.3. Fingerprint IDs/biometric identifiers

39.d.3j. Store identifying numbers including, but not limited to:

39.d.3j.1. State ID numbers

39.d.3j.2. Driver license numbers

39.d.3j.3. Social Security numbers

39.d.3j.4. FBI numbers

39.d.3j.5. OCA/JOCA numbers

39.d.3j.6. Passport numbers

39.d.3j.7. Military IDs

39.d.3j.8. Other agency identifiers

39.d.3k. Maintain current and historical addresses.

39.d.3l. Maintain current and historical telephone numbers.

39.d.3m. Maintain email addresses and social media identifiers.

39.d.3n. Occupation / Employment

39.d.3o. Store photographs and mugshots.

39.d.3p. Associate warrants, arrests, citations, incidents, field interviews, and investigative cases.

39.d.3q. Display known associates and organizational affiliations.

39.d.3r. Track gang affiliations and intelligence information.

39.d.3s. Support person-to-person relationship tracking.

39.d.3t. Identify potential duplicate persons using configurable matching algorithms.

39.d.3u. Provide comprehensive person history views.

39.d.3v. The RMS should allow marking of sensitive individuals (e.g., confidential informants, juveniles) and restrict access accordingly.

39.e. The Master Vehicle Index Module shall maintain a centralized repository of vehicles encountered by the agency and do the following:

- 39.e.1. Create and maintain a unique master vehicle record.
- 39.e.2. Link to Incident Report for stolen or recovered status.
- 39.e.3. Capture vehicle information including, but not limited to:
 - 39.e.3a. License plate
 - 39.e.3b. VIN
 - 39.e.3c. State of registration
 - 39.e.3d. Year
 - 39.e.3e. Make
 - 39.e.3f. Model
 - 39.e.3g. Body Style
 - 39.e.3h. Color
 - 39.e.3i. Body type
 - 39.e.3j. Type of Vehicle
- 39.e.4. Store vehicle ownership information.
- 39.e.5. Maintain registration history.
- 39.e.6. Track vehicle status information.
- 39.e.7. Associate vehicles with, but not limited to:
 - 39.e.7a. Persons
 - 39.e.7b. Organizations
 - 39.e.7c. Incidents
 - 39.e.7d. Cases
 - 39.e.7e. Citations
 - 39.e.7f. Crashes
 - 39.e.7g. Arrests
 - 39.e.7h. Traffic Stops
- 39.e.8. Track vehicle modifications and distinguishing characteristics.
- 39.e.9. Store vehicle-related intelligence notes.
- 39.e.10. Support multiple plates associated with a vehicle over time.

39.e.11. Maintain historical ownership and registration records.

39.e.12. The RMS should allow for linking of multiple individuals (owners, drivers, passengers) to a single vehicle record.

39.e.13. Detect duplicate vehicle records.

39.e.14. The RMS should track vehicle status (e.g., stolen, impounded, recovered, evidence).

39.e.15. Support integration with state motor vehicle systems.

39.e.16. Maintain vehicle photographs.

39.f. The Master Location Index Module shall maintain a centralized repository of addresses, facilities, landmarks, and geographic locations. Module should support integration with MNPd GIS system and do the following:

39.f.1. Create and maintain unique master location records.

39.f.2. Support:

39.f.2a. Street addresses

39.f.2b. Apartment/suite/unit number (if applicable)

39.f.2c. Intersections

39.f.2d. Mile Marker references

39.f.2e. Geo-coordinates (latitude/longitude, X/Y)

39.f.2f. Spatial queries (e.g., find incidents within X feet of a location)

39.f.2g. Common name/business name (e.g., "Cumberland River Park Condominiums", "The Batman Building")

39.f.2h. Location type classification (residence, business, school, park, etc.)

39.f.2i. Premise hazard flags (e.g., officer safety warnings, previous incidents)

39.f.3. Validate addresses using GIS and addressing databases.

39.f.4. Provide map-based search and analysis capabilities.

39.f.5. Support GIS mapping integration.

39.f.6. Associate locations with, but not limited to:

39.f.6a. Incidents

39.f.6b. Calls for service

39.f.6c. Warrants

39.f.6d. Cases

39.f.6e. Persons

39.f.6f. Organizations

39.f.6g. Property

39.f.7. Track occupancy and ownership history.

39.f.8. Support geofencing, hot spot mapping, and proximity alerts.

39.f.9. Display location activity history.

39.f.10. Identify repeat locations and chronic problem locations.

39.f.11. Support parcel identification numbers.

39.f.12. Allow attachment of photographs, diagrams, and documents.

39.f.13. Module should support integration with NCIC/NLETS and TN/local data sources for location-based alerts or warrant checks, where applicable.

39.f.14. MNPD currently utilizes an external Address Validation Web Service. Module should provide equivalent address validation functionality and indicate whether this capability is extendible to interfaces beyond the RMS.

39.g. The Master Property Index Module shall maintain a centralized repository of property and assets documented by the agency and do the following:

39.g.1. Create and maintain unique master property records.

39.g.2. Support tracking of, but not limited to:

39.g.2a. Stolen property

39.g.2b. Recovered property

39.g.2c. Seized property

39.g.2d. Found property

39.g.2e. Safekeeping property

39.g.2f. Evidentiary property

39.g.3. Capture detailed descriptions including, but not limited to:

39.g.3a. Property type/ Category (e.g., electronics, firearms, jewelry, narcotics)

39.g.3b. Brand

39.g.3c. Model

39.g.3d. Serial number/manufacture ID

39.g.3e. Color

39.g.3f. Condition

39.g.3g. Container

39.g.3h. Estimated Value

39.g.4. Support property classification standards.

39.g.5. Associate property with, but not limited to:

39.g.5a. Owners

39.g.5b. Possessors

39.g.5c. Suspects

39.g.5d. Victims

39.g.5e. Cases

39.g.5f. Incidents

39.g.5g. Evidence records

39.g.6. Track chain-of-custody relationships.

39.g.7. Maintain property status history.

39.g.8. Detect duplicate property records.

39.g.9. Support barcode(Code 39), QR Code and RFID technologies.

39.g.10. The RMS should support bulk property entry for inventory management.

39.g.11. Maintain photographs and supporting documentation.

39.g.12. Support integration with evidence management systems.

39.g.13. Provide complete historical ownership tracking.

39.g.14. Support firearm-specific data elements.

39.g.15. The RMS should support property disposition workflows and inventory audit capabilities.

39.g.16. The RMS should allow the same item to be associated with multiple records if applicable (e.g., repeat offenses).

39.h. The Master Organization Index Module shall maintain a centralized repository of businesses, government entities, schools, non-profit organizations, gangs, and other organizations and do the following:

39.h.1. Create and maintain unique master organization records.

39.h.2. Support organization types including, but not limited to:

- 39.h.2a. Businesses
- 39.h.2b. Government agencies
- 39.h.2c. Educational institutions
- 39.h.2d. Religious organizations
- 39.h.2e. Non-profit organizations
- 39.h.2f. Financial institutions
- 39.h.2g. Criminal organizations
- 39.h.2h. Gangs

39.h.3. Capture organizational information including, but not limited to:

- 39.h.3a. Organization name
- 39.h.3b. Alternate names
- 39.h.3c. DBA names
- 39.h.3d. Physical and mailing address(es)
- 39.h.3e. Tax identifiers
- 39.h.3f. Licensing or registration information
- 39.h.3g. Primary Contact information

39.h.4. Maintain multiple locations associated with an organization.

- 39.h.4a. Allow for multiple primary contacts associated with an organization.

39.h.5. Associate organizations with, but not limited to:

- 39.h.5a. Persons
- 39.h.5b. Vehicles
- 39.h.5c. Locations
- 39.h.5d. Incidents
- 39.h.5e. Investigations
- 39.h.5f. Permits
- 39.h.5g. Licenses

39.h.6. Track ownership and management history.

- 39.h.7. Support organization hierarchy structures.
- 39.h.8. Track organizational affiliations and partnerships.
- 39.h.9. Maintain intelligence and investigative notes.
- 39.h.10. Identify duplicate organizations.
- 39.h.11. Display organization activity history.
- 39.h.12. Support document and attachment storage.
- 39.h.13. Maintain historical records of organizational changes.
- 39.h.14. Support regulatory and compliance tracking.

12. **40. Mental Health Interaction Module**

40.a. The proposed RMS should include a dedicated Mental Health Interaction Module to document, track, and analyze law enforcement encounters involving individuals experiencing mental or behavioral health crises. This module must support MNPd efforts in crisis response, de-escalation, diversion, and community collaboration. It should be compliant with applicable privacy regulations, including HIPAA and 42 CFR Part 2: Use and disclosure of substance use disorder patient records, and enable data-driven decision-making for both operational and strategic planning.

40.b. The module should also incorporate capabilities for managing Crisis Intervention Team (CIT) reports, Behavioral Health interactions, special populations encounters, and Wellness or Welfare Checks as core components of comprehensive response to individuals in crisis.

40.c. Module should allow for the creation and management of mental health-related incident reports independently or in conjunction with other RMS modules (e.g., CAD, incident reports, response to resistance, case management).

40.d. Module should integrate with or link to person records, enabling officers to view historical interactions with individuals exhibiting mental health concerns.

40.e. Module should provide secure access control to sensitive mental health data, configurable by user role and permissions.

40.f. Module should support both proactive and reactive documentation, including welfare checks, crisis calls, and co-responder deployments.

40.g. Module should allow tagging of incidents as "mental health-related," "CIT," "behavioral health," "special populations," or "welfare check" for classification and reporting.

40.h. Officers should be able to document behaviors observed, level of crisis, perceived threats, and de-escalation tactics used.

40.i. Module should include fields for CIT officer involvement, including CIT certification status, response outcomes (e.g., voluntary transport, involuntary commitment, arrest, referral), and any response to resistance applied.

40.j. The RMS should support standardized classifications such as:

40.j.1. Suicidal ideation or attempt

40.j.2. Psychosis or hallucinations

40.j.3. Substance use-related mental health issues

40.j.4. Intellectual or developmental disability concerns

40.k. Officers should be able to indicate if a co-responder or behavioral health professional was involved and document their role and follow-up actions.

40.l. The RMS should support the documentation of Behavioral Health issues, including dual diagnoses, cognitive impairments, and medication-related concerns.

40.m. The module should allow the identification of special populations, including, but not limited to:

40.m.1. Individuals with developmental disabilities

40.m.2. Elderly persons with dementia or cognitive decline

40.m.3. Persons experiencing homelessness

40.m.4. Persons with residence insecurity

40.m.5. Veterans with PTSD or service-related conditions

40.m.6. Juveniles (Extra level of security)

40.n. Module should support structured documentation for Wellness or Welfare Checks, including request source, reason for the check, observed conditions, and final disposition.

40.o. Module should allow attachment of relevant digital files, including body-worn camera footage, medical transport documentation, referral forms, and photos.

40.p. Module should support linking mental health-related incidents to specific individuals, enabling identification of frequent contacts or high-risk individuals.

40.q. The RMS should display prior mental health interactions - including CIT, welfare checks, and behavioral health contacts - when viewing a person record (with access restrictions in place).

40.r. Module should allow agencies to configure behavioral flags or alerts for officer safety, visible during CAD dispatch or field-based record lookup.

40.s. The RMS should support the ability to view trends and patterns across repeated interactions, supporting early intervention or diversion efforts.

40.t. Module should provide access controls to limit mental health-related records to authorized personnel only.

40.u. The RMS should be configurable to comply with HIPAA, 42 CFR Part 2, and local/state privacy laws.

40.v. The RMS should maintain full audit trails of access and changes to mental health records.

40.w. Role-based access should be enforced, and user actions logged to support compliance audits.

40.x. Module should support documentation of referrals or collaborations with external partners, including, but not limited to:

- 40.x.1. Crisis response teams
- 40.x.2. Hospitals or psychiatric facilities
- 40.x.3. Mobile mental health units
- 40.x.4. Social service providers

40.y. Where appropriate and legally permissible, the RMS should enable secure data exchange or notifications with designated partner agencies or diversion programs.

40.z. Module should allow tracking of outcomes from external referrals.

40.aa. Module should support user-defined reporting on mental health-related incidents, including trends over time, frequency by individual or location, and co-responder outcomes.

40.ab. Reports should be able to be filtered by classification type (e.g., CIT, behavioral health, welfare check, special population).

40.ac. Dashboards should provide visual analytics on mental health calls, response to resistance in mental health incidents, repeat contacts, and geographical hotspots.

40.ad. The RMS should support exporting data in common formats (e.g., PDF, CSV, Excel) for internal and external reporting requirements.

40.ae. Reports should support program evaluation for initiatives such as CIT, mobile crisis response, jail diversion, and social services referrals.

40.af. Module should be fully accessible via mobile devices for in-field data entry.

40.ag. The mobile interface should support rapid selection of predefined behaviors, threat levels, and de-escalation tactics.

40.ah. Officers should be able to complete CIT reports, welfare check summaries, or behavioral health documentation in the field.

40.ai. The RMS should allow offline functionality with secure synchronization once connectivity is restored.

40.aj. MNPd should be able to configure behavior categories, mental health classifications, response options, referral agencies, and form templates to meet local needs.

40.ak. The module should support user-defined fields for additional data capture specific to local programs, partnerships, or legal requirements.

40.al. Workflow customization should be available to support review, approval, or supervisor notification processes.

40.am. MNPd should be able to configure CIT-specific workflows or follow-up assignments, such as review by behavioral health teams or re-engagement units.

41. Metro Citations Module

- 41.a. Module should be fully integrated with other RMS components (e.g., person records, CAD, case management, property, court) to avoid data duplication and ensure consistency.
- 41.b. Module should be compliant with all applicable federal, TN, and local laws and standards regarding citation issuance and reporting.
- 41.c. Module should be accessible through both desktop and mobile platforms for use in the field and in the office.
- 41.d. Module should allow searching and filtering by citation number, violator name, license plate, officer, date, location, or violation type.
- 41.e. Module should provide audit trails for all citation record changes including timestamps and user IDs.
- 41.f. The module should interface with external systems including, but not limited to:
 - 41.f.1. Module should interface with the Traffic Violation Information System (TVIS) for Nashville courts.
 - 41.f.2. Module should allow the import of citations from third-party platforms.
- 41.g. Module should support all Metro-required citation forms and data fields.
- 41.h. Module should provide automated reporting of citation statistics to state agencies where required.
- 41.i. Module should support user-defined reporting and dashboards (e.g., citation trends by location or violation type).
- 41.j. Module should support printing and exporting of reports including, but not limited to: Excel, CSV, PDF.
- 41.k. Module should allow for scheduled or ad hoc reporting on citation activity.
- 41.l. Officers should have access only to citations he or she issued unless higher access is granted.
- 41.m. Module should maintain a full audit trail of all user activity related to citations.
- 41.n. Module should allow for user-defined fields as needed by MNPd.

42. Missing Persons Module

- 42.a. The proposed RMS should include a fully integrated Missing Person Module that supports the end-to-end documentation, tracking, alerting, and resolution of missing person reports. The module should enable rapid response, secure information sharing, and compliance with local, TN, and federal mandates, including NCIC missing person categories and timelines.
- 42.b. The RMS should include a dedicated Missing Person Module integrated with the Master Person Index, Incident, Case, and BOLO modules.
- 42.c. Module should support the creation, update, and closure of missing person records.
- 42.d. Each missing person report should be assigned a unique identifier and associated with a primary incident or case number.
- 42.e. Module should allow tracking of investigative actions, leads, contacts, and inter-agency

communications.

42.f. Module should support multiple types of missing person classifications as defined by NCIC and MNPd.

42.g. Module should support the following missing person classifications (at minimum):

42.g.1. Juvenile

42.g.2. Endangered (e.g., mental illness, disability, elderly)

42.g.3. Involuntary (e.g., abduction, foul play)

42.g.4. Catastrophe victim

42.g.5. Other (e.g., voluntary, unknown)

42.h. Each missing person entry should allow flags for:

42.h.1. AMBER Alert eligibility

42.h.2. Silver Alert eligibility

42.h.3. Suspected human trafficking

42.h.4. Repeat or chronic missing person

42.i. Module should allow MNPd administrators to define additional custom categories and alert types.

42.j. Module should allow entry of comprehensive details, including, but not limited to:

42.j.1. Full name, aliases, nicknames

42.j.2. DOB, age, gender at birth, race, ethnicity

42.j.3. Physical descriptors (height, weight, eye/hair color, scars, tattoos, etc.)

42.j.4. Clothing worn, personal items, medical needs

42.j.5. Photograph(s) and supporting documents

42.j.6. Last known location, time, and circumstances

42.j.7. Reporting party information

42.k. Module should support entry of multiple leads, sightings, and follow-up notes.

42.l. Users should be able to track investigative actions taken and assign tasks or case responsibilities to specific personnel.

42.m. Module should support case status updates (e.g., Open, Recovered, Located, Deceased, Closed).

42.n. Module should support real-time or batch submission of missing person entries to NCIC via TN message switch (as applicable).

42.o. Module should automatically flag records requiring NCIC entry and track compliance timelines.

- 42.p. Module should support NCIC-required fields and include validation before submission.
- 42.q. Users should be able to update, cancel, or clear NCIC entries from within the RMS (subject to CJIS security protocols).
- 42.r. Module should log all NCIC submissions, changes, and status updates for auditing.
- 42.s. Module should allow automatic creation of a BOLO when an officer submits for approval a missing person report.
- 42.t. Module should allow alerts to be sent internally (via RMS), externally (email/text), or to integrated CAD/Mobile systems.
- 42.u. Module should support the generation of flyers or bulletins with MNPB branding and approved templates.
- 42.v. Module should allow configuration of alert expiration dates/times and alert level (e.g., Critical, High, Routine).
- 42.w. Alerts should include photo(s), physical description, last known location, and case contacts.
- 42.x. Module should support advanced search functionality across all missing person records by:
- 42.x.1. Name, alias, DOB, physical descriptors
 - 42.x.2. Classification, alert level, status
 - 42.x.3. Last known location or address
 - 42.x.4. Case number or incident number
- 42.y. Users should be able to search open and closed missing person records.
- 42.z. Search results should support drill-down into full missing person profiles and linked incident/case data.
- 42.aa. The module should allow geotagging of the last known location and related sightings or leads.
- 42.ab. Users should be able to view missing person reports on an integrated map interface.
- 42.ac. Module should support radius-based search and mapping of similar cases (e.g., within 5 miles, 30 days).
- 42.ad. Module should allow the linking of missing person cases to areas known for human trafficking, runaways, or vulnerable populations.
- 42.ae. Sensitive records (e.g., human trafficking victims, child custody cases) should have elevated privacy controls and audit trails.
- 42.af. Module should log all access, changes, and exports of missing person data for CJIS compliance.
- 42.ag. Administrators should be able to configure access rules by user role, unit, or assignment.
- 42.ah. Module should support reporting on active and resolved missing person cases, including demographics, classifications, resolution types, and durations.

- 42.ai. Module should generate compliance reports on NCIC entry timelines and alert issuance.
- 42.aj. Users should be able to generate statistical reports by date, district, status, and type of missing person.
- 42.ak. Reports should be exportable in PDF, Excel, and CSV formats, and support schedule delivery.
- 42.al. Module should support optional data sharing with other jurisdictions, fusion centers, and missing persons clearing houses.
- 42.am. Users should be able to mark a record as shareable or restricted.
- 42.an. Module should support integration with public-facing portals for public awareness (if desired by MNPd).
- 42.ao. Module should support export/import of missing person data in standard formats (e.g., NIEM, XML, JSON).
- 42.ap. Administrators should be able to configure classification types, alert templates, and report formats.
- 42.aq. Module should allow review and reclassification of historical missing person reports.
- 42.ar. Module should support the merging of duplicate missing person entries and audit trail of data corrections.
- 42.as. Module should include quality control tools to flag incomplete or inconsistent entries.
- 42.at. In MNPd's current RMS, the Incident and Missing Person modules are closely integrated. In the new RMS we would like to have the Missing Person module independent of the Incident module by having all relevant data also in the Missing Person module.

43. Mobile Field Reporting Module

- 43.a. The proposed RMS should include a fully integrated, secure, and user-friendly Mobile Field Reporting Module that enables law enforcement personnel to access, create, edit, and submit reports and other records from the field using mobile devices such as laptops, tablets, or smartphones. This module is critical to improving officer efficiency, accuracy, situational awareness, and real-time data sharing. It is MNPd's desire that this RMS module will replace our current internally developed Automated Field Reporting system.
- 43.b. The Mobile Field Reporting Module provides authorized users with full or role-based access to RMS functions from mobile or in vehicle devices.
- 43.c. The Mobile Field Reporting Module supports the use and expansion of custom fields based on the needs of MNPd.
- 43.d. The Mobile Field Reporting Module supports the easy creation of new forms for field-based entry by MNPd as needed.
- 43.e. The Mobile Field Reporting Module supports the creation, editing, and submission of the following, but not limited to:

- 43.e.1. Incident reports

- 43.e.2. Arrest reports
- 43.e.3. Metro Citations
- 43.e.4. Field interview (FI) reports
- 43.e.5. Supplementals and follow-up reports
- 43.e.6. Witness and victim statements
- 43.f. The module should allow users to:
 - 43.f.1. Copy or auto-populate fields from CAD data or previous records
 - 43.f.2. Attach photos, sketches, audio, and video files directly from the field
 - 43.f.3. Capture signatures for appropriate electronic forms
 - 43.f.4. Capture fingerprint to apply to appropriate electronic forms (e.g., State Misdemeanor Citation).
 - 43.f.5. Use dropdowns, auto-fill, and validation rules to ensure consistency
 - 43.f.6. Utilize voice-to-text dictation if supported by the device
 - 43.f.7. Allow real-time or store-and-forward submission of reports, depending on connectivity.
 - 43.f.8. Allow users to utilize dark mode monitor display.
- 43.g. The module should support offline data entry when connectivity is unavailable, with the ability to:
 - 43.g.1. Store reports securely on the device
 - 43.g.2. Automatically sync data with the RMS once a connection is restored
 - 43.g.3. Queue uploads and handle conflict resolution for concurrent changes
- 43.h. Display active and historical CAD incidents for assigned units
- 43.i. Allow officers to initiate reports from CAD call data
- 43.j. Include dispatch details such as:
 - 43.j.1. Call type, location, date/time
 - 43.j.2. Unit assignments
 - 43.j.3. Caller information
 - 43.j.4. Officer safety alerts and comments
- 43.k. Auto-link field reports to CAD event numbers and dispatch narratives
- 43.l. Enable officers to search and retrieve information in the field, including:

- 43.l.1. Incident and case reports
- 43.l.2. Arrests and booking records
- 43.l.3. Warrants and protective orders
- 43.l.4. Field interviews and citations
- 43.l.5. Person, vehicle, property, and address records
- 43.m. Display relationships (e.g., linked cases, associated persons, gang affiliations)
- 43.n. Provide real-time alerts for warrants, flags, BOLOs, and safety warnings
- 43.o. Enforce strong security measures, including, but not limited to:
 - 43.o.1. Device authentication
 - 43.o.2. Secure user login with multi-factor authentication (MFA)
 - 43.o.3. Full encryption of data in transit and at rest
- 43.p. Should comply with CJIS Security Policy and applicable federal, TN, and local data protection laws
- 43.q. Automatically lock sessions after inactivity and allow remote wipe for lost or compromised devices
- 43.r. Support modern web browsers and native apps on devices including, but not limited to:
 - 43.r.1. Windows 11 laptops and tablets
 - 43.r.2. iOS smartphones and tablets
- 43.s. Interface should be responsive and optimized for both touch and keyboard/mouse interaction
- 43.t. Support hands-free or in-vehicle use cases (where safe and legal)
- 43.u. Minimize the number of clicks/taps required for common report writing tasks
- 43.v. Allow officers to:
 - 43.v.1. Save reports as draft
 - 43.v.2. Submit for supervisor review
 - 43.v.3. Receive corrections or return notices from supervisors
 - 43.v.4. Final approval by Records / Booking. Records sends clarifying review.
 - 43.v.5. Provide tracking of report status (e.g., draft, pending review, approved)
- 43.w. Include notification or alert features for returned or rejected reports
- 43.x. Support customizable, pre-configured report templates/forms for various incident types

43.y. Allow quick entry using templates for:

- 43.y.1. DUI
- 43.y.2. Domestic violence
- 43.y.3. Vehicle accidents
- 43.y.4. Theft, burglary, assault, etc.

43.z. Support MNPD-specific checklists, code tables, and policy compliance prompts

43.aa. Allow capture and attachment of:

- 43.aa.1. Digital photos (with time/date/GPS stamping)
- 43.aa.2. Videos and audio recordings
- 43.aa.3. Sketches, diagrams, and scanned documents

43.ab. Support QR code/barcode scanning (e.g., driver's licenses, VIN, property tags) to run query via Message Switch. Populate results from scan into form or screen.

43.ac. Automatically link uploaded media to the associated report or case file

43.ad. Notify officers of:

- 43.ad.1. Reports pending review or correction
- 43.ad.2. System updates or policy changes
- 43.ad.3. CAD call assignments or updates (if integrated with CAD)
- 43.ad.4. BOLOs or critical alerts (e.g., missing persons, officer safety issues)

43.ae. Display GIS-based maps for:

- 43.ae.1. Assigned calls for service
- 43.ae.2. Recent crime activity in the area
- 43.ae.3. Locations of interest (e.g., flagged addresses, probationers)

43.af. Allow geotagging of reports and evidence from the field

43.ag. Integrate with AVL/GPS systems for officer safety and situational awareness (if available)

43.ah. Scalable to support multiple users with high availability

43.ai. Provide secure, managed mobile application deployment via MDM (Mobile Device Management), if applicable

43.aj. Include tools for IT administrators to:

- 43.aj.1. Monitor device sync status

43.aj.2. Push updates

43.aj.3. Manage permissions remotely

43.ak. Log all report submissions, edits, and deletions

43.al. Track user access to mobile RMS features and data

43.am. Allow supervisors or internal affairs to audit mobile activity by user/device.

43.an. The Metropolitan Nashville Police Department (MNPd) utilizes standardized XPS Field Reports as official documentation in our daily operations. These forms are directly aligned with our current Automated Field Reporting (AFR) desktop application and Records Management System (RMS). We are providing these PDF forms to ensure that your proposed RMS solution can accurately capture and support all data fields contained within them (see attached MNPd RFP RMS Field Reports_v.2026). Moving forward MNPd wants the Field Reports to be printed as PDFs not XPS.

43.ao. While many fields reflect standard data collected by most law enforcement agencies, MNPd also employs several custom fields that are essential and should be preserved in any future solution.

43.ap. It is MNPd's strong preference that all fields from the current reports be fully incorporated into the new RMS, Field Reporting Module without loss of functionality or data fidelity.

Attachments:

File Name or URL	Type	Description
MNPd RFP RMS Field Reports_v.2	File	

13. **44. Police Fleet Records Management Module**

44.a. The RMS should store a master record for each vehicle in the fleet.

44.b Each vehicle record should include:

44.b.1. Unique vehicles will have an ID (automatically assigned or customizable) (e.g.. boats, trailers, ATV, Golf Cart, etc.)

44.b.2. Make, model, and year

44.b.3. VIN (Vehicle Identification Number)

44.b.4. License plate number

44.b.5. Departmental Unit/Assignment

44.b.6. Vehicle type (e.g., patrol, unmarked, K-9, SWAT, transport)

44.b.7. Color and markings

44.b.8. Radio ID, GPS/AVL ID, MDC/Computer ID

44.b.9. Acquisition date and source (editable purchase/lease/grants/funding sources)

44.b.10. Status (active, in maintenance, retired, totaled, etc.)

44.c. Module should track:

44.c.1. Assigned officers or units (historical and current)

44.c.2. Usage logs including, but not limited to:

44.c.2a. Date/time of use

44.c.2b. Officer(s) using vehicle

44.c.2c. Starting and ending mileage

44.c.2d. Shift or call log association

44.d. Optional: Integration with dispatch/CAD system for automated usage logging.

44.e. Module should support:

44.e.1. Scheduled maintenance tracking (oil changes, tire rotations, inspections)

44.e.2. Repair history

44.e.3. Service provider details

44.e.4. Parts used, labor hours, and cost

44.e.5. Support for importing/exporting service data from fleet maintenance systems (optional API support).

44.f. Module should allow entry of:

44.f.1. Fuel type and amount

44.f.2. Fueling location

44.f.3. Date/time of fueling

44.f.4. Mileage at time of fueling

44.f.5. Support for MPG tracking and efficiency reports

44.g. Module should record incidents involving vehicles and link them to an Incident Report including, but not limited to:

44.g.1. Traffic collisions

44.g.2. Vandalism, theft, or damage

44.g.3. Internal/external investigation references

44.g.4. Repair or insurance follow-up

44.h. Module should support the generation of reports such as:

44.h.1. Vehicle inventory reports by type, assignment, or status

- 44.h.2. Maintenance due/past due reports
- 44.h.3. Usage by officer/unit
- 44.h.4. Fuel usage trends
- 44.h.5. Cost of ownership per vehicle
- 44.h.6. Audit logs for all vehicle record modifications
- 44.h.7. Funding Source

44.i. All changes to vehicle records should be logged with user ID, timestamp, and reason for change (audit trail)

44.j. Module should support integration with:

- 44.j.1. CAD systems for vehicle dispatch data
- 44.j.2. GPS/AVL systems for real-time tracking
- 44.j.3. Maintenance management systems
- 44.j.4. Fuel card systems
- 44.j.5. Asset and inventory management modules

44.k. Module should track the full lifecycle of each vehicle:

- 44.k.1. Acquisition
- 44.k.2. Assignment
- 44.k.3. Maintenance history
- 44.k.4. Incidents
- 44.k.5. Decommission/retirement
- 44.k.6. Disposal or auction data

45. Property and Evidence Management Module

45.a. The RMS Property and Evidence Module shall provide a secure, auditable, and CJIS-compliant system for the intake, tracking, storage, analysis, transfer, and disposition of all property and evidence collected by MNPD. The module must support the full lifecycle of evidence while maintaining an unbroken chain of custody and integration with related RMS, CAD, and forensic systems.

45.b. The system shall support the management of all property and evidence types, including but not limited to:

- 45.b.1. Firearms and weapons

- 45.b.2. Ammunition
- 45.b.3. Controlled substances (drugs and narcotics)
- 45.b.4. Currency and financial instruments
- 45.b.5. General property and valuables
- 45.b.6. Digital and electronic evidence (metadata support)
- 45.b.7. Biological evidence
- 45.b.8. Latent fingerprints and impressions

45.c. The module shall be fully integrated with the RMS case, incident, arrest, and person records.

45.d. The system shall provide real-time status tracking of property and evidence from intake through final disposition.

45.e. The system shall maintain a complete, immutable audit trail for all actions.

45.f. The system shall allow property and evidence intake directly from:

- 45.f.1. Incident reports
- 45.f.2. Arrest records
- 45.f.3. Field submissions from mobile field use (MNPd Form 110)

45.g. Intake records shall capture, at minimum:

- 45.g.1. Incident number
- 45.g.2. Date and time of collection
- 45.g.3. Collecting officer
- 45.g.4. Location of collection
- 45.g.5. Evidence/Property type and category
- 45.g.6. Detailed description
- 45.g.7. Make, model, color
- 45.g.8. Quantity, weight, and units
- 45.g.9. Packaging type
- 45.g.10. Condition at intake
- 45.g.11. Associated persons (suspect, victim, owner)

45.h. The system shall support barcode, QR Code, and/or RFID assignment at intake.

45.i. The system shall support detailed tracking of firearms and weapons, including, but not limited to:

- 45.i.1. Make, model, caliber/gauge
- 45.i.2. Serial number (with validation and duplicate detection)
- 45.i.3. Firearm type (handgun, rifle, shotgun, etc.)
- 45.i.4. National Crime Information Center (NCIC) firearm indicators
- 45.i.5. Condition and safety status (loaded/unloaded)

45.j. The system shall support linkage to:

- 45.j.1. Associated ammunition
- 45.j.2. Ballistics and forensic records
- 45.j.3. ATF-required reporting fields

45.k. The system shall support firearm disposition options, including, including, but not limited to:

- 45.k.1. Return to owner
- 45.k.2. Destruction
- 45.k.3. Transfer
- 45.k.4. Court-ordered disposition

45.l. The system shall support drug evidence tracking by:

- 45.l.1. Drug type and classification
- 45.l.2. Estimated and confirmed weight
- 45.l.3. Packaging method
- 45.l.4. Field test results
- 45.l.5. Laboratory analysis results

45.m. The system shall support:

- 45.m.1. Multiple weigh-ins
- 45.m.2. Weight change tracking
- 45.m.3. Bulk and individual packaging

45.n. The system shall support scheduled and witnessed destruction with electronic certification.

45.o. The system shall support intake and tracking of currency and financial instruments, including, but not limited to:

45.o.1. Cash (recorded by denomination and total amount)

45.o.2. Checks

45.o.3. Gift cards

45.o.4. Foreign

45.o.5. Counterfeit

45.o.6. Other negotiable instruments

45.p. The system shall support:

45.p.1. Dual verification for currency counts

45.p.2. Association to forfeiture cases

45.p.3. Deposit and transfer tracking

45.q. The system shall generate reconciliation and audit reports.

45.r. The system shall support intake and tracking of general property, including, including, but not limited to:

47.r.1. Electronics

47.r.2. Jewelry

47.r.3. Documents

47.r.4. Miscellaneous items

45.s. The system shall support property ownership tracking and return authorization.

45.t. The system shall support the intake and management of latent fingerprints and impressions, including, including, but not limited to:

45.t.1. Latent prints

45.t.2. Palm prints

45.t.3. Footwear impressions

45.t.4. Tool marks

45.u. Latent fingerprint records shall capture:

45.u.1. Method of collection

45.u.2. Surface type

45.u.3. Location collected

45.u.4. Associated case and item

- 45.u.5. Collector and technician information
- 45.v. The system shall support:
 - 45.v.1. Linkage to AFIS and biometric systems
 - 45.v.2. Status tracking (submitted, analyzed, matched, no hit)
 - 45.v.3. Association with laboratory results and reports
- 45.w. The system shall allow storage of images, metadata, and examiner notes.
- 45.x. The system shall automatically track and document:
 - 45.x.1. Every transfer of custody
 - 45.x.2. Date, time, location, and personnel involved
 - 45.x.3. Reason for transfer
 - 45.x.4. Produce tracking receipt.
- 45.y. The system shall prevent unauthorized transfers.
- 45.z. The system shall support electronic signatures and acknowledgments.
- 45.aa. Manage temporary checkouts including, but not limited to:
 - 45.aa.1. Lab analysis.
 - 45.aa.2. Courtroom presentation.
 - 45.aa.3. Review by external agencies.
- 45.ab. Require justification, return date, and auto-reminders for overdue items.
- 45.ac. MNPD is interested if there is a way to interface this module with our Laboratory Information Management System (LIMS) named JusticeTrax by Versaterm. Allowing for evidence logged in at the Property room can be seamlessly transferred into the lab's LIMS system and then back to the property room.
- 45.ad. The system shall support configurable storage hierarchies, including, including, but not limited to:
 - 45.ad.1. Facilities
 - 45.ad.2. Rooms
 - 45.ad.3. Lockers
 - 45.ad.4. Shelves and bins
- 45.ae. The system shall track current and historical storage locations.
- 45.af. The system shall support evidence holds and court-ordered restrictions.

45.ag. The system shall support disposition workflows, including, including, but not limited to:

- 45.ag.1. Return to owner
- 45.ag.2. Court-ordered release
- 45.ag.3. Destruction
- 45.ag.4. Auction or forfeiture

45.ah. The system shall require appropriate authorization and documentation prior to disposition.

45.ai. The system shall retain permanent disposition history.

45.aj. The system shall provide standard and ad hoc reports, including, but not limited to:

- 45.aj.1. Inventory reports
- 45.aj.2. Audit and compliance reports
- 45.aj.3. Chain-of-custody reports
- 45.aj.4. Firearms and drug-specific reports

45.ak. Reports shall be exportable in common formats including, but not limited to: PDF, Excel, CSV.

45.al. The system shall integrate with:

- 45.al.1. RMS core modules
- 45.al.2. CAD systems
- 45.al.3. Digital evidence systems
- 45.al.4. DCSO Jail Management System
- 45.al.5. Forensic and laboratory systems
- 45.al.6. AFIS and biometric systems
- 45.al.7. NCIC and state reporting systems (where permitted)
- 45.al.8. eTrace Direct interfaces
- 45.al.9. NESS+ interfaces

45.am. The system shall comply with:

- 45.am.1. FBI CJIS Security Policy
- 45.am.2. TN and federal evidence handling regulations
- 45.am.3. Applicable retention laws

45.an. The system shall support:

45.an.1. Data encryption at rest and in transit

45.an.2. Configurable retention schedules

45.an.3. Configuration, Scalability, and Usability

45.ao. The system shall provide a configurable, intuitive user interface.

46. Response to Resistance (Use of Force) Reporting Module

46.a. The Response to Resistance module should be a fully integrated component of the RMS.

46.b. Module should comply with applicable local, TN, and federal reporting standards (e.g., FBI National Response to Resistance/Use-of-Force Data Collection).

46.c. The Response to Resistance module should support multiple types of force used, including but not limited to:

46.c.1. Physical force

46.c.2. OC spray

46.c.3. TASER/ECD

46.c.4. Baton

46.c.5. Firearm

46.c.6. Canine deployment

46.c.7. Less lethal projectiles

46.c.8. Edged Weapon

46.c.9. Vehicle

46.c.10. Other (with freeform textbox for details)

46.d. Module should allow for configurable approval workflows for Response to Resistance incidents based on MNPDP policy (e.g., officer to supervisor to MNPDP command staff to internal affairs).

46.e. Module should include a Response to Resistance (RTR) form (MNPDP forms 108 and 108T) and process, fully integrated into Response to Resistance reporting. This process should document both officer actions and subject behavior, with emphasis on proportionality and de-escalation efforts.

46.f. All data should be auditable, with complete logging of changes (who, what, when).

46.g. Module should support the creation of a new Response to Resistance report or link to an existing incident or arrest report.

46.h. Module should capture and link the following information:

- 46.h.1. RMS generated Control Number with ability to create prefix labeling of the Control Numbering
- 46.h.2. Master Name Record or if applicable, Unknown Suspect Record
- 46.h.3. Officer(s) involved
- 46.h.4. Subject(s) involved
- 46.h.5. Type(s) of resistance used
- 46.h.6. Subject behavior/threat level
- 46.h.7. Officer's justification for response to resistance
- 46.h.8. Location, date, and time of incident
- 46.h.9. Injuries to officers and/or subjects
- 46.h.10. Medical treatment provided or refused
- 46.h.11. Witnesses (officer and civilian)
- 46.h.12. Supervisory review notes
- 46.i. Module should support the Response to Resistance form, including structured fields and narrative sections to capture:
 - 46.i.1. Subject resistance level(s) (e.g., passive, active, assaultive, deadly)
 - 46.i.2. Officer response type(s) and rationale for escalation
 - 46.i.3. Timeline and sequence of resistance vs. response
 - 46.i.4. De-escalation tactics attempted
 - 46.i.5. Effectiveness of each force application
- 46.j. Module should allow attachment of relevant documents, images, audio, and video (e.g., body-worn camera footage, photos of injuries).
- 46.k. Module should allow creating a report for an officer that has to euthanize an animal (e.g. deer or dog).
- 46.l. Module should support capturing data through structured fields as well as narrative text.
- 46.m. Module should allow for multi-officer and multi-subject scenarios, each with independent force details.
- 46.n. Users should be able to indicate whether the force used was effective or ineffective.
- 46.o. Module should support a configurable, multi-level approval workflow (e.g., Officer to Sergeant to Lieutenant to Internal Affairs).
- 46.p. Notifications and reminders should be generated for outstanding or overdue reviews.

- 46.q. Approvers should be able to approve, reject, or request revisions to reports.
- 46.r. Module should support the routing of reports to different divisions, such as Response to Resistance Review Boards or Professional Standards/Internal Affairs and Behavioral Health.
- 46.s. The RTR form should be visible and reviewable at each stage of the workflow.
- 46.t. The Response to Resistance module should integrate with the following RMS modules:
 - 46.t.1. Incident Reports
 - 46.t.2. Arrests
 - 46.t.3. Case Management
 - 46.t.4. HR Module/Personnel
- 46.u. Module should automatically cross-reference relevant report numbers (e.g., incident, arrest, CAD).
- 46.v. Module should link to officer training and certification records (e.g., defensive tactics, Taser certification) to validate qualifications.
- 46.w. Integration with CAD and body-worn camera systems is preferred for timeline correlation.
- 46.x. The RTR form data should be available for internal and external reporting, and cross referenced in associated modules.
- 46.y. Module should provide configurable dashboards and statistical reports, including but not limited to:
 - 46.y.1. Types and frequency of force used
 - 46.y.2. Demographics of subjects involved
 - 46.y.3. Time, location, and geographic mapping of incidents
 - 46.y.4. Trends by officer, shift, or division
 - 46.y.5. Comparison of use-of-force to arrest or call volume
 - 46.y.6. Officer responses (from RTR data)
- 46.z. All reports should be exportable to common formats including, but not limited to: PDF, Excel, CSV.
- 46.aa. Module should support ad-hoc querying and report creation by authorized users.
- 46.ab. Module should support NIBRS/TIBRS-compliant reporting and submission to external entities (e.g., FBI Response to Resistance/Use-of-Force database).
- 46.ac. TIBRS Zero Report capabilities
- 46.ad. Officers may only access Response to Resistance reports they are authorized to view.
- 46.ae. Supervisors and MNPd command staff may have broader access based on roles and permissions.
- 46.af. Internal Affairs or designated oversight users should have full access for auditing and investigative

purposes.

46.ag. Sensitive information should be protected from unauthorized disclosure (e.g., medical details, juvenile involvement).

46.ah. RTR forms and fields must be secured with the same level of access controls as Response to Resistance reports.

46.ai. Module should maintain a complete audit trail of all RTR reports, including, but not limited to:

46.ai.1. Date/time stamps

46.ai.2. User actions (create, edit, approve, delete)

46.ai.3. Comments and feedback from supervisors

46.aj. Module should support records retention in compliance with applicable legal and policy requirements.

46.ak. Archived reports should remain accessible for legal inquiries or historical review.

46.al. Changes to RTR form data must be included in the audit trail.

46.am. Module should allow officers to initiate or complete Response to Resistance reports in the field via mobile devices (tablet, MDC).

46.an. Mobile field reports should sync securely with the central RMS when connectivity is restored.

46.ao. The RTR form should be mobile-optimized for structured and narrative entry during or immediately following incidents.

47. RMS Security Module

47.a. The proposed RMS should include a comprehensive Security Module. The module should allow for precise control over permissions and access rights over individual records to ensure only authorized personnel can view, edit, or delete sensitive law enforcement data, in compliance with CJIS, HIPAA, and local data protection policies.

47.b. The Security Module should support centralized management, audit logging, and administrative tools for maintaining security integrity across all RMS components.

47.c. The module should include a centralized Security Module integrated across all RMS components, including but not limited to: Person Records, Cases, Incidents, BOLOs,

47.d. The module should support MNPD-wide, Group-based, and Individual User access controls.

47.e. The module should allow for hierarchical permission structures, enabling access inheritance and overrides.

47.f. All access and permission assignments should be fully auditable, with historical tracking of changes and activities.

47.g. The module should support single sign-on (SSO), Multi-Factor authentication, and compliance with CJIS authentication requirements.

47.h. The module should allow administrators to create, modify, deactivate, and delete user accounts securely.

47.i. Each user account should include:

47.i.1. Username and secure password

47.i.2. Role(s) and group membership

47.i.3. Last login time and IP address

47.j. Module should support enforcement of AD compliance password complexity, expiration, and lockout rules based on MNPDP policy.

47.k. Administrators should be able to force logout or temporarily disable user accounts for security reasons.

47.l. Module should allow the creation and management of user Groups, based on unit, division, assignment, or function (e.g., Detectives, Records, Patrol, Administration).

47.m. Permissions may be applied at the Group level to simplify access control management.

47.n. Users may belong to multiple Groups with appropriate permissions merged or overridden as configured.

47.o. Module should allow Group-based restrictions on data visibility (e.g., only Homicide Unit can view Homicide case files).

47.p. Module should support record-level security, allowing access to be restricted to:

47.p.1. Specific users

47.p.2. Specific groups

47.p.3. Specific agencies (in multi-agency systems)

47.q. Module should allow record and field-level access restrictions, e.g., hiding sealed juvenile information from unauthorized users.

47.r. Module should support "Need to Know" flags or case sensitivity markers for sensitive investigations.

47.s. Supervisors, or their assigned designee, should be able to mark certain records as "Confidential" or "Restricted" with granular access control.

47.t. In multi-agency environments, the module should ensure that data is segregated by MNPDP, unless explicitly shared.

47.u. Administrators should be able to control which agencies or users can view shared or regional records.

47.v. Module should log all access to shared records and enforce tagging or labeling of cross agency data.

47.w. Module should maintain a complete, immutable audit trail of all access and activity within the RMS.

47.x. The audit log should record:

47.x.1. User ID

- 47.x.2. Action taken (e.g., viewed, edited, deleted)
- 47.x.3. Module and record ID affected
- 47.x.4. Date/time stamp
- 47.x.5. IP address or terminal ID
- 47.y. Audit logs should be accessible only to authorized personnel and protected from tampering or deletion.
- 47.z. Module should support audit reports by user, module, date range, or action type.
- 47.aa. Data redaction tools for partial visibility based on role or case sensitivity.
- 47.ab. Time-bound access (e.g., temporary access to specific records for a set duration).
- 47.ac. Module should prevent concurrent logins unless explicitly permitted by policy.
- 47.ad. Module should include an administrative dashboard to manage user access, roles, groups, and permissions.
- 47.ae. Bulk user management tools should be available (e.g., batch assign roles, deactivate accounts).
- 47.af. Module should support scheduled reviews of user access rights and role assignments.
- 47.ag. Module should provide built-in alerts for security-related anomalies (e.g., multiple failed logins, unusual access patterns).
- 47.ah. The Security Module should comply with:
 - 47.ah.1. CJIS Security Policy v6.0
 - 47.ah.2. HIPAA, when applicable
- 47.ai. Module should support full auditability and encryption of sensitive data at rest and in transit.
- 47.aj. Offeror should provide documentation of security certifications and compliance upon request.
- 47.ak. The module should support the generation of reports such as:
 - 47.ak.1. User login history
 - 47.ak.2. Access to restricted cases or records
 - 47.ak.3. Permission changes over time
 - 47.ak.4. Inactive user accounts
- 47.al. Administrators should be able to configure automatic security alerts and compliance reminders.
- 47.am. Active Directory (AD) integration.
- 47.an. Importing of AD Groups and assigning rights.

47.ao. Delegated Administration for large agencies with multiple divisions.

47.ap. Provide a self-service portal for users to request access changes.

48. Offender Registry Module

48.a. The proposed RMS should include a fully integrated Offender Registry Module to enable MNPd to manage, monitor, and report information related to registered offenders in full compliance with federal and TN laws, including the Adam Walsh Child Protection and Safety Act, SORNA, Savanna's Law (Repeat Domestic Abuse Offender), Animal Abuse Registry Tennessee Drug Offender Registry, and other applicable mandates.

48.b. The module should ensure timely registration, updates, public notifications, inter-agency communication, and secure data management of all registered offenders under the MNPd's jurisdiction. This module should include all the requirements outlined herein.

48.c. Allow for the creation, editing, and management of offender records.

48.d. Track all legally required data fields, including, but not limited to:

48.d.1. Full name, aliases, DOB, SSN, physical descriptors

48.d.2. Link to Master Name Index

48.d.3. Residential, employment, and school addresses

48.d.4. Date of registration and registration duration

48.d.5. Offense(s) requiring registration, conviction details, and statute codes

48.d.6. Risk level/tier classification

48.d.7. Vehicle information

48.d.8. Phone numbers, email addresses, online identifiers

48.d.9. Photographs

48.d.10. Fingerprints and palm prints

48.d.11. Integrate with DCSO's NEC AFIS Live Scan fingerprint systems.

48.e. Track registration status (Active, Non-compliant, Incarcerated, Relocated, and Deceased)

48.f. Support documentation of registration updates, verifications, absconders, and compliance checks.

48.g. Comply with:

48.g.1. Sex Offender Registration and Notification Act (SORNA)

48.g.2. Adam Walsh Child Protection and Safety Act

48.g.3. Tennessee Sex Offender Registry

- 48.g.4. CJIS security policy
- 48.g.5. Savanna's Law (Repeat Domestic Abuse Offender)
- 48.g.6. Tennessee Drug Offender Registry
- 48.g.7. Tennessee Animal Abuse Registry

48.h. Ensure compliance with mandated registration timelines (e.g., initial registration, periodic updates, in-person appearances).

48.i. Allow configuration of registration and reporting rules by jurisdiction.

48.j. Support in-person registration process at the Davidson County Sherriff's Office including, but not limited to:

- 48.j.1. Photo capture and attachment
- 48.j.2. Signature collection
- 48.j.3. Address verification
- 48.j.4. Documentation of legal notices and acknowledgments
- 48.j.5. Track and schedule:
- 48.j.6. Annual verification appointments
- 48.j.7. In-person appearances (based on tier)
- 48.j.8. Upcoming expiration or renewal dates

48.k. Generate automated alerts and reminders for:

- 48.k.1. Upcoming registration deadlines
- 48.k.2. Missed appointments (non-compliance)
- 48.k.3. Community notification requirements

48.l. Support public notification workflows including, but not limited to:

- 48.l.1. Neighborhood alerts
- 48.l.2. Email bulletins
- 48.l.3. Public-facing registry updates (if applicable)

48.m. The module should integrate with:

- 48.m.1. TN Sex Offender Registry systems for data sharing and synchronization
- 48.m.2. National Sex Offender Registry (NSOR) and NSOPW
- 48.m.3. Jail/Booking Module to update status (e.g., incarcerated/released)

- 48.m.4. Court Management Systems for automatic updates upon conviction
- 48.m.5. Warrant and Compliance Tracking Modules for enforcement
- 48.m.6. Public website portals (as allowed by MNPD policy)
- 48.n. Advanced search and filter options including, but not limited to:
 - 48.n.1. Name, alias, DOB
 - 48.n.2. Physical address (with map view or radius search)
 - 48.n.3. Employer or school
 - 48.n.4. Offense type/statute
 - 48.n.5. Compliance status
- 48.o. Ability to generate maps of registered offenders in a given area.
- 48.p. Search for offenders with upcoming verifications or expired registrations.
- 48.q. Generate standard and ad hoc reports including, but not limited to:
 - 48.q.1. Active vs. non-compliant offenders
 - 48.q.2. Upcoming registration verifications
 - 48.q.3. Offender movement and relocation tracking
 - 48.q.4. Community notification logs
- 48.r. Export reports in Excel, PDF, and CSV formats.
- 48.s. Schedule automatic report generation and delivery to designated personnel.
- 48.t. Full audit trail of all actions taken on offender records including, but not limited to:
 - 48.t.1. Edits, updates, and deletions
 - 48.t.2. User who performed the action
 - 48.t.3. Timestamp of changes
- 48.u. Track history of address changes, compliance checks, and status updates.
- 48.v. Allow for flagging and review of non-compliant offenders.
- 48.w. Generate audit logs and compliance reports for internal or external review.
- 48.x. If applicable, support publishing a public-facing version of the sex offender registry that includes:
 - 48.x.1. Approved offender details per law

48.x.2. Mapping interface for public to search by location

48.x.3. Risk level indicators

48.x.4. Exclusion of protected or sealed data

48.y. Allow MNPd controlled redaction or suppression of sensitive information (e.g., juveniles, victims, protected identities).

48.z. Support for offline field use (e.g., for compliance checks), with sync upon reconnection.

48.aa. Intuitive, user-friendly interface for entering and updating data.

48.ab. High-resolution photo management and storage.

48.ac. Support data import and migration from legacy systems.

49. Traffic Stop Module

49.a. The RMS should include a comprehensive Traffic Stop Module designed to document, manage, search, and report all law enforcement vehicle stops in compliance with federal, state, and local reporting requirements. The module shall support officer safety, data accuracy, transparency, supervisory review, and public accountability. The RMS shall allow users to create and maintain a complete traffic stop record, including but not limited to:

49.a.1. Date and time of stop (start and end)

49.a.2. Location of stop (address, intersection, GPS coordinates, precinct)

49.a.3. Ability to force location.

49.a.4. Reason for stop (selectable from agency-defined lists)

49.a.5. Stop type (traffic, investigative, checkpoint, etc.)

49.b. Vehicle information: License plate number and state

49.c. Driver information:

49.c.1. Date of birth, gender, race

49.c.2. Driver's license number and issuing state

49.c.3. Zip Code

49.d. Ability to capture incomplete driver data, driver's licenses, VIN, and other information that the officer can then use to efficiently fill out reports.

49.e. Officer(s) involved, including primary and assisting officers

49.f. Patrol unit information

49.g. The RMS shall support both manual data entry and auto-population from integrated systems where available.

49.h. The Traffic Stop Module shall document enforcement actions and outcomes, including:

- 49.h.1. Warnings
- 49.h.2. Citations (with citation linkage)
- 49.h.3. Incident and arrests (with arrest report linkage)
- 49.h.4. Consent to Search asked
- 49.h.5. Searches conducted if approved
- 49.h.6. Search type (vehicle, person, consent, probable cause, inventory, etc.)
- 49.h.7. Basis for search
- 49.h.8. Search results
- 49.h.9. Seizures (property, contraband, evidence)
- 49.h.10. Fleeing/Evading the Traffic Stop

49.i. Each action shall be timestamped and associated with the responsible officer.

49.j. The RMS shall support the capture of demographic data as required by applicable laws or agency policy, including:

- 49.j.1. Race and ethnicity
- 49.j.2. Gender
- 49.j.3. Age range (if exact age unavailable)

49.k. The module shall support bias-based policing data collection and enable reporting consistent with state and federal mandates.

49.l. The Traffic Stop Module shall integrate seamlessly with:

- 49.l.1. Metro and State Citation and eCitation systems
- 49.l.2. CAD (Computer-Aided Dispatch)
- 49.l.3. Body-worn camera and in-car video systems (linking CFS)

49.m. The RMS shall prevent duplicate data entry by sharing common data elements across modules.

49.n. The RMS shall support configurable workflows, including, but not limited to:

- 49.n.1. Draft, submitted, approved, and rejected statuses
- 49.n.2. Audit trails capturing all changes, approvals, and rejections

49.o. The RMS shall provide robust search and reporting capabilities, including:

- 49.o.1. Search by demographic, vehicle, officer, date range, location, or outcome
- 49.o.2. Advanced filtering and Boolean search options
- 49.o.3. Predefined and ad hoc reports
- 49.o.4. Export of reports in standard formats including, but not limited to: PDF, CSV, Excel
- 49.p. Statistical and trend analysis (e.g., stops by location, evades, officer, or demographic group)
- 49.q. The Vehicle Stop Module shall be fully accessible from mobile devices and MDCs, allowing officers to:
 - 49.q.1. Create and edit vehicle stop records in the field
 - 49.q.2. Operate in online and offline modes with synchronization
 - 49.q.3. Use dropdowns, validation rules, and minimal typing for efficiency

50. Trespass Waivers Module

- 50.a. The proposed RMS should include a Trespass Waivers Module that allows law enforcement personnel to accept waivers submitted by property owners or authorized representatives, granting officers the authority to enforce trespassing laws on their behalf, especially during non-business hours or when the property is unoccupied. The module should provide tools to track waiver status, enforce time limits, associate waivers with locations, and allow integration with incident and arrest reporting.
- 50.b. Module should include a dedicated Trespass Waivers Module integrated with the Master Location Index and other relevant modules (e.g., Incident, Case, BOLO).
- 50.c. Module should support entry, update, renewal, and expiration of trespass waivers for both residential and commercial properties. (1 Year)
- 50.d. Each waiver should be uniquely identified and associated with a specific physical address or parcel.
- 50.e. Module should allow waivers to be linked to businesses, owners, property managers, or other authorized agents, stored in the Master Name Index.
- 50.f. Waivers should include status indicators (e.g., Active, Expired, Pending Review).
- 50.g. The module should allow users to enter key details of a waiver, including, but not limited to:
 - 50.g.1. Property address and location ID
 - 50.g.2. Property type (e.g., residential, commercial, vacant lot)
 - 50.g.3. Owner or agent name and contact info
 - 50.g.4. Waiver start and end dates
 - 50.g.5. Hours of enforcement (e.g., after business hours)
 - 50.g.6. Any conditions or restrictions (e.g., no entry without signs)
- 50.h. Module should allow the attachment of digital waiver forms, property maps, contact letters, and

photos.

50.i. Module should support electronic or scanned signature capture for waiver approval and legal compliance.

50.j. Module should allow for bulk entry or renewal of waivers for property owners managing multiple locations.

50.k. The module should support search and filtering of trespass waivers by:

50.k.1. Address or parcel ID

50.k.2. Owner or agent name

50.k.3. Date of expiration or renewal

50.k.4. Property type or zone

50.k.5. Waiver status

50.l. Module should allow users to view all waivers on an interactive map interface with filtering by status and type.

50.m. Each waiver record should allow drill-down access to related incidents, citations, arrests, or field contacts at that location.

50.n. Module should allow configuration of default waiver durations (e.g., 6 or 12 months) and automatic expiration handling.

50.o. Property Owners should receive automated reminders when a waiver is approaching expiration (e.g., 30, 15, and 5 days prior).

50.p. Module should support a renewal workflow, including review of prior waiver terms and property activity.

50.q. Expired waivers should be archived but remain searchable for historical and legal reference.

50.r. Module should alert users when an officer or unit is dispatched or responding to a location with an active trespass waiver.

50.s. Officers should be able to confirm waiver status from mobile or in-field devices (via CAD or mobile RMS interface).

50.t. Waiver data should integrate with Incident, Arrest, and Field Interview modules to document enforcement actions.

50.u. Module should allow citation and arrest records to be linked directly to the relevant trespass waiver record.

50.v. Module should support optional integration with patrol check or extra-duty officer modules to increase visibility of waiver properties.

50.w. Module should allow configurable alerts for properties with active trespass waivers, viewable by field units.

50.x. Waivers may include officer safety notes (e.g., known squatters, hazardous conditions, prior violent encounters).

50.y. Trespass alerts should appear when addresses are queried or populated in RMS modules (e.g., Incident, Arrest, CAD call).

50.z. The module should support an optional web-based portal for property owners or managers to:

- 50.z.1. Submit new waiver requests

- 50.z.2. Upload required documents and signatures

- 50.z.3. Track waiver status and expiration

- 50.z.4. Request renewals

- 50.z.5. Ability to email expiration notification alerts

50.aa. Module should support reports showing:

- 50.aa.1. Active waivers by zone, property type, or expiration date

- 50.aa.2. Properties with frequent trespass enforcement actions

- 50.aa.3. Officers or units assigned to waiver enforcement

- 50.aa.4. Waiver submission and renewal trends over time

50.ab. Reports should be exportable including, but not limited to: PDF, Excel, or CSV formats.

50.ac. Module should support scheduled or on-demand reporting for MNPd command staff, city attorneys, or public records compliance.

50.ad. Access to the Trespass Waivers Module should be controlled by role-based security profiles.

50.ae. Only authorized personnel should be able to approve or deactivate waivers.

50.af. Sensitive waiver details (e.g., private property owner contact info) should be protected by appropriate user permissions.

50.ag. All actions (creation, edits, deletions, views) should be logged and auditable.

50.ah. Administrators should be able to configure:

- 50.ah.1. Default waiver durations

- 50.ah.2. Required fields and documents

- 50.ah.3. Notification schedules and templates

- 50.ah.4. Waiver conditions and classifications

50.ai. Public portal entries should be reviewed and approved by designated MNPd personnel before activation.

50.aj. Module should allow batch processing and mass renewal notifications.

50.ak. Module should support import/export of waiver data from legacy systems or for interagency sharing.

51. Vehicle Pursuit Module

51.a. The Vehicle Pursuit module should be a fully integrated component of the RMS, with seamless interaction with other RMS relevant modules.

51.b. Module should comply with local, TN, and federal standards for pursuit documentation and reporting (e.g., CALEA, TN-specific pursuit reporting requirements).

51.c. Module should support multiple officers, vehicles, and jurisdictions participating in a single pursuit event.

51.d. All actions should be auditable and logged, including data entry, edits, and approvals.

51.e. Module should allow for configurable workflows based on MNP policy (e.g., Officer to Supervisor to RMS to Command Review to Internal Affairs).

51.f. Module should support creating a standalone vehicle pursuit report and linking to existing CAD, incident, or arrest reports.

51.g. The module should capture the following key data elements:

51.g.1. Date and time pursuit was initiated and terminated

51.g.2. Initiating officer(s) and unit(s)

51.g.3. Participating officers, supervisors, and agencies

51.g.4. Location(s) of pursuit start, end, and significant events

51.g.5. Reason for initiating the pursuit (e.g., traffic offense, felony)

51.g.6. Subject vehicle information (make, model, color, plate, VIN if available)

51.g.7. Pursued suspect(s) information (if known or apprehended)

51.g.8. Speeds, road, weather, and traffic conditions

51.g.9. Pursuit duration and distance

51.g.10. Tactical maneuvers used (e.g., PIT, spike strips)

51.g.11. Injuries, fatalities, or property damage (civilian, suspect, officer)

51.g.12. Termination method (e.g., suspect stopped, officer terminated, crash)

51.g.13. Supervisory notifications and involvement

51.h. Module should support structured data fields and narrative descriptions.

51.i. Module should allow officers to attach supporting media (e.g., dashcam footage, photos, diagrams).

51.j. Module should be configurable to allow classification of pursuits as "compliant," "non-compliant," or "unauthorized" per MNPDP policy.

51.k. Module should support customizable, multi-level approval workflows (e.g., Officer to Sergeant to Lieutenant to Pursuit Review Board).

51.l. Module should provide automated notifications/reminders for outstanding reviews.

51.m. Supervisors should be able to review, comment, approve, reject, or request modifications.

51.n. Module should support routing of pursuit reports to Internal Affairs, Behavioral Health or risk management when applicable.

51.o. The Vehicle Pursuit module should integrate with the following RMS components:

- 51.o.1. CAD (Computer-Aided Dispatch)

- 51.o.2. Incident Reports

- 51.o.3. Arrest Records

- 51.o.4. Response to Resistance Reports

- 51.o.5. Internal Affairs/Professional Standards/Behavioral Health

- 51.o.6. Training Records

- 51.o.7. Officer Profile

51.p. Module should allow the linking of pursuit events to related reports (e.g., arrest, accident, response to resistance).

51.q. Integration with AVL/GPS systems and in-car camera systems is preferred for corroborating location and timeline data.

51.r. The module should support generation of standard and custom pursuit-related reports, including, but not limited to:

- 51.r.1. Number of pursuits by officer, shift, unit, or division

- 51.r.2. Reasons for pursuits

- 51.r.3. Outcomes and termination methods

- 51.r.4. Injuries and property damage statistics

- 51.r.5. Duration, distance, and time-of-day trends

- 51.r.6. Pursuits involving interagency coordination

51.s. Module should provide dashboards for supervisory and MNPDP staff review.

51.t. Reports should be exportable in formats including, but not limited to: PDF, Excel, and CSV.

51.u. Module should support submission of data to TN or federal agencies as required (e.g., for statewide pursuit databases).

51.v. Officers may only view or edit their own pursuit reports prior to submission.

51.w. Officers may only view or edit their own submitted pursuit reports if not approved by a supervisor.

51.x. Supervisors and authorized personnel should have access to reports for their areas of responsibility.

51.y. Internal Affairs, Risk Management, or designated oversight roles should have full access for audit and review purposes.

51.z. The module should maintain a complete audit log of all actions related to pursuit records, including, but not limited to:

51.z.1. Creation, editing, and deletion

51.z.2. Approval history

51.z.3. User IDs and timestamps

51.aa. Module should support data retention policies based on legal and regulatory requirements.

51.ab. Archived reports should remain accessible for administrative review, legal discovery, or historical trend analysis.

51.ac. Module should allow field personnel to initiate or complete pursuit documentation from mobile data terminals MDTs or MDC tablets.

51.ad. Data should be securely synchronized with the central RMS when connectivity is restored.

14. **52. Training**

52.a. Any RMS training conducted should ensure maximum accessibility to all end users and training effectiveness.

52.b. Training should enable MNPd officers and staff to confidently navigate and operate the RMS in their respective roles. RMS End User training will make up the majority of training required at MNPd and will require flexibility for scheduling the training sessions.

52.c. Offeror will provide training materials, user guides, and administrator documentation for the life of the contract.

52.d. MNPd prefers Instructor-Led Training for its RMS users.

52.e. MNPd plans to develop two (2) fully qualified MNPd RMS Master Subject Matter Experts (SMEs) capable of supporting, training, troubleshooting, and advising on all aspects of the Records Management System (RMS). The Offeror shall provide an extensive training plan for the SMEs, starting as early as possible in the RMS implementation process. This unique training opportunity provides for comprehensive End-to-End training on the RMS, necessary for the MNPd SMEs to be able to deliver expert-level RMS support before the Go-Live of the RMS.

52.f. Training instruction across MNPd should cover the full RMS lifecycle, including but not limited to:

52.f.1. User workflows and functional modules

52.f.2. Administrative functions and permissions

52.f.3. Data management, security settings, and audit features

52.f.4. Reporting, analytics, and dashboards

52.f.5. RMS updates, releases, and maintenance operations

52.f.6. Detailed walkthroughs of all RMS processes

52.f.7. Scenario-based, hands-on training

52.g. Offeror should provide training on all the functionalities which should include but not be limited to the following:

52.g.1. Productivity and performance metrics

52.g.2. Audit logs and compliance reporting

52.g.3. Handling system errors and edge cases

52.g.4. Escalation procedures

52.g.5. Support and ticketing processes

52.h. Offeror should provide train-the-trainer training which should focus on teaching methodology, RMS usage, shortcuts, and troubleshooting basics in addition to providing a solid hands-on learning experience for:

52.h.1. System and Database Administrators

52.h.2. MNPd Master Subject Matter Experts (SMEs)

52.h.3. MNPd Field Training Officers (FTOs)

52.h.4. MNPd Patrol Precinct RMS Power Users

52.h.5. MNPd Department RMS Power Users

52.h.6. MNPd Training Academy RMS Trainers

52.h.7. Records Department Personnel

52.h.8. MNPd IT Support Personnel

52.h.9. RMS System and Database Administrators

52.i. Offeror should provide comprehensive training that equips MNPd's technical staff to:

52.i.1. Operate and maintain all RMS components

52.i.2. Troubleshoot common system issues

52.i.3. Perform account administration tasks (e.g., adding/modifying/deleting users, resetting

passwords, managing permissions)

52.i.4. Provide Administrators with copies of all Troubleshooting guides

52.j. Records training shall focus on records-centric workflows and compliance-driven tasks required to support accurate, timely, and legally compliant records management. Training should enable Records personnel to efficiently perform their duties within the RMS and serve as subject-matter resources for records-related processes. Training for Records Department users should include, but not be limited to:

52.j.1. Records intake, review, validation, and configurable approval workflows

52.j.2. Report correction, rejection, supplementation, and version control

52.j.3. Records linking, case updates, and cross-referencing (persons, vehicles, property, incidents)

52.j.4. Data quality assurance, auditing, and error resolution

52.j.5. Compliance with state and federal reporting requirements (e.g., NIBRS/TIBRS, UCR statutory retention rules)

52.j.6. Records release, redaction, expungement, and sealing processes, as applicable

52.j.7. Use of RMS search, reporting, and query tools for records management and public/internal requests

52.j.8. Training should emphasize accuracy, consistency, legal compliance, and efficient handling of high-volume records operations.

52.k. MNPd identifies continuous learning opportunities as desirable for training new users to the RMS and for when RMS users change roles at MNPd.

52.l. Access to any training material and resources must be maintained throughout the contract period.

52.m. Offeror shall grant MNPd the ability to reproduce and internally distribute unlimited additional copies of all documentation and training materials at no additional cost.

52.n. Offeror shall permit MNPd to make audio and video recordings of any training sessions for later use at no additional cost to MNPd.

52.o. The Offeror shall provide comprehensive support-related materials throughout life of the contract which should including, but not limited to:

52.o.1. Technical support procedures

52.o.2. Escalation protocols

52.o.3. RMS maintenance and troubleshooting documentation

52.o.4. Configuration and deployment guides

52.o.5. Application Programming Interface (API) or integration documentation

52.o.6. Ongoing support and updates to accommodate changes in legislation or MNPd policy should be included.

Numbering between 53 and 58 are reserved by Metro if needed as part of future scope modifications.

59. RMS – Interface Connectivity

59.a Offeror must have the ability to migrate connectivity of all existing interfaces from the current RMS to the newly implemented RMS. Offeror must conduct an inventory all existing external and internal interfaces connected to the current RMS. Offeror must document each interface's functionality, protocols, frequency of use, data formats, and endpoints. Offeror must assess the compatibility of these interfaces with the proposed RMS platform prior to implementation.

59.b. Offeror will conduct an inventory of all MNPD interfaces connected to the RMS.

59.c. Offeror must ensure that the new RMS supports replication or enhancement of all existing interface capabilities.

59.d. Offeror shall develop, implement and maintain an interface migration plan that has been approved by MNPD.

59.e. Where applicable, the Offeror must:

59.e.1. Map data structures from the legacy RMS to the new RMS interface schemas.

59.e.2. Provide documentation on any data transformations required.

59.e.3. Validate data integrity and completeness post-migration.

59.f. Throughout the life of the contract the offeror is expected to disclose any licensing, development toolkits, or middleware required for future integrations.

59.g. Interfaces must meet security and privacy standards consistent with industry's best practices and regulatory compliance, including, but not limited to:

59.g.1. Data encryption in transit and at rest.

59.g.2. Audit logging of data exchanges.

59.g.3. Compliance with applicable standards (e.g., CJIS, HIPAA).

59.h. Offeror should create and execute Interface Test Plans (ITPs) for each interface.

59.i. Offeror should provide validation reports confirming functionality and performance benchmarks.

59.j. Offeror should deliver complete documentation for:

59.j.1. Each migrated interface (technical specs, API references, configuration guides).

59.j.2. Standard Operating Procedures (SOPs) for ongoing interface maintenance.

59.k. Provide training to designated IT personnel on interface management and troubleshooting.

59.l. Offer should provide post-implementation support for the term of the contract to:

59.l.1. Monitor and address any interface-related issues.

59.l.2. Optimize performance and resolve errors.

59.l.3. Update or reconfigure interfaces as needed due to changes in upstream/downstream systems.

59.m. The RMS should allow for future modification or expansion of interfaces without proprietary restrictions.

59.n. Offeror is responsible for coordinating with third-party vendors/agencies as needed to ensure seamless migration of interconnected systems (e.g., CAD, DCSO JMS, Davidson County Court Systems, RMS data exchanges with state/federal databases). There are currently thirty-four (34) MNPd Current Interfaces with Metro's current police records management system which are as follows:

59.n.1. NEC Multiple Biometric Identification System (MBIS) Fingerprint Identification System

59.n.1a. Offeror will create interfaces necessary to perform MBIS functionality to customer's existing client/server RMS functionality.

59.n.1b. Direction: Bi-Directional

59.n.1c. Module: Arrest/Booking

59.n.1d. Format: XML/Text File

59.n.1e. Exchange: Web Service

59.n.2. GovCIO (ATS) Message Switch

59.n.2a. Offeror will provide capabilities for the GovCIO ATS Message switch similar to what is provided for the client/server RMS version of the switch. Provide a way to send/receive messages related to TBI/NCIC/TIES systems. As well as the queries to local RMS.

59.n.2b. Direction: Bi-Directional

59.n.2c. Module/Systems: Arrest/Booking/Master Name/Court Documents/NEC MBIS (fingerprints)/ DataWorks Plus Version 5.165 (Mugshots)/Justice Information Systems/Juvenile Court/Davidson County Sheriff Department

59.n.2d. Format: XML

59.n.2e. Exchange: Web Service

59.n.3. Automated Field Reporting (AFR) Interface

59.n.3a. Imports data captured in electronic forms from officers in the field.

59.n.3b Direction: Import

59.n.3c. Module: Incident, Arrest, Court Document, Field Interview, Evidence, etc.

59.n.3d. Format: XML

59.n.3e. Exchange: Web Service

59.n.4. DataWorks Plus PhotoManager - Version 5.165 Booking/Mugshot/Fingerprint System

59.n.4a. Offeror will create an interface that will send XML for individual arrests with demographic information to DataWorks. Then, it will receive xml messages to import the mugshot and/or SMTs, and the single fingerprint into the RMS (attach them to the arrest or juvenile contact record.) The single fingerprint is required for the finalized arrest report.

59.n.4b. Direction: Bi-Directional

59.n.4c. Module: Arrest/Booking

59.n.4d. Format: XML, JPG

59.n.4e. Exchange: Web Service

59.n.5. DataWorks Plus PhotoManager Version 5.165 – ID Card System

59.n.5a. Offeror will create an interface that will retrieve information from employee module, then it will return the photograph and the date of card printed.

59.n.5b. Direction: Bi-Directional

59.n.5c. Module: Employee

59.n.5d. Format: Text, JPG

59.n.5e. Exchange: Web Service

59.n.6. ATF eTrace Direct

59.n.6a. Offeror will create an interface that sends data from RMS into the ATF's eTrace site for weapons stolen/found/recovered received by RMS. The Trace information for the weapon is downloaded periodically.

59.n.6b. Direction: Bi-Directional

59.n.6c. Module: Evidence

59.n.6d. Format: JSON

59.n.6e. Exchange: Web Service

59.n.7. ATF NESS+

59.n.7a. Offeror will create an interface that will monitor a directory for delimited files provided by the ATF NESS+ system.

59.n.8. Oracle Fusion Cloud 26.Q (HR)

59.n.8a. Offeror will create an interface that will monitor a directory for delimited files provided by the Oracle Fusion Cloud 26.Q (HR) system. When files are found, the interface will create/update employee data accordingly in the RMS system.

59.n.8b. Direction: 1-Way Import into RMS

59.n.8c. Module: Human Resources/Personnel

59.n.8d. Format: Delimited

59.n.8e. Exchange: File Share

59.n.9. Interface with DCSO Jail Management System

59.n.9a. Offeror will create interfaces necessary to perform DCSO JMS functionality to customer's existing client/server RMS functionality. MNPd transmits initial booking information as well as finalization files including demographics, alias, and charges (warrants).

59.n.9b. DCSO is currently implementing the Executive Information Services JMS

59.n.9c. Direction: Bi-Directional

59.n.9d. Module: Arrest/Booking

59.n.9e. Format: XML

59.n.9f. Exchange: FTP

59.n.10. Interface with Motorola CAD System

59.n.10a. Offeror will create an interface that imports the calls for service involving MNPd resources. The interface creates an entry on the Calls for Service and Incident tables (RMS)

59.n.10b. Direction: 1-Way Import into RMS

59.n.10c. Module: Calls for Service, Incident

59.n.10d. Format SQL View

59.n.10e. Exchange: Database Query to CAD system

59.n.11. State Criminal Justice Information System

59.n.11a. Offeror will create interfaces necessary to perform CJIS functionality to customer's existing client/server RMS functionality. MNPd sends initial booking file as well as completed bookings files including demographic, alias, and charges. MNPd receives files with new warrants (charges), dispositions, bond conditions. This interface connects the RMS to the Justice Integration Services (JIS) department which supports the state criminal courts in the Criminal Court clerk of Metropolitan Nashville and Davidson County. The JIS platform is formerly known as the criminal justice information system (CJIS). This system name should not be confused with the FBI's CJIS Security Policy, which is unrelated.

59.n.11b. Direction: Bi-Directional

59.n.11c. Module: Arrest/Booking

59.n.11d. Format: XML/Text File

59.n.11e. Exchange: FTP

59.n.12. State Juvenile Justice Information System (JIMS) (The vendor is Quest.)

59.n.12a. Offeror will create interfaces necessary to perform JIMS functionality to customer's existing client/server RMS functionality. The files sent to Juvenile Justice Information include demographic information, alias, and charges. We do receive Juvenile charges dispositions.

59.n.12b. Direction: Bi-Directional

59.n.12c. Module: Arrest/Booking

59.n.12d. Format: XML/Text File

59.n.12e. Exchange: FTP

59.n.13. Carfax Crash Reports

59.n.13a. Exports accident reports daily excluding fatalities and reports that include any citation/violation. No additional redactions.

59.n.13b. Direction: 1-Way export Accidents

59.n.13c. Module: Accident

59.n.13d. Format: XML

59.n.13e. Exchange: SFTP

59.n.14. Tennessee Medical Examiner Office

59.n.14a. List of documents (PDF, DOC, DOCX) for incidents related to death, aggravated assault, or DUI NIBRS Codes: (09A-09C, 13A, 640, 680, 685, 690, 695, 90D)

59.n.14b. Direction: 1-Way export incident reports

59.n.14c. Module: Incident, Case Management

59.n.14d. Format: ZIP File: of PDF, DOC, DOCX, TXT

59.n.14e. Exchange: SFTP

59.n.15. THORplus/Crimetracer Interface

59.n.15a. Offeror will create interfaces necessary to provide RMS information since 1/1/2009 excluding incidents with sex crime offense. Any incident that has a juvenile victim will show redacted information as well as an empty comments' field. This is handled via SQL views. They include many tables present currently on RMS (50+).

59.n.15b. The data is pulled directly from RMS via appliance software installed on a MNPD server.

59.n.15c. Direction: Export

59.n.15d. Module: Incident, Arrest, Court Documents

59.n.15e. Format: SQL Views

59.n.15f. Exchange: Stored procedures on Crime Tracer appliance

59.n.16. TITAN Interface for Records

59.n.16a. Description: Exports accident reports daily excluding fatalities and reports that include any citation/violation. There are additional redactions to the data: insurance information (addresses, driver license info, etc.)

59.n.16b. Direction: 1-Way export Accidents

59.n.16c. Module: Accident

59.n.16d. Format: XML

59.n.16e. Exchange: File system

59.n.17. LexisNexis Crash Reports

59.n.17a. Exports daily accident reports. The fatalities and reports containing violations are excluded.

59.n.17b. Direction: 1-Way export Accidents

59.n.17c. Module: Accident

59.n.17d. Format: PDF, JPEG, XML

59.n.17e. Exchange: SFTP

59.n.18. LexisNexis Minor Crashes

59.n.18a. Description: Retrieves the Minor Accident reports completed via LexisNexisRisk DORS Self-Service application by citizens. It is not currently imported into RMS.

59.n.18b. Direction: 1-Way Import Minor Crashes

59.n.18c. Module: SQL Table

59.n.18d. Format: XML

59.n.18e. Exchange: SFTP

59.n.19. LexisNexis Citizen Reports

59.n.19a. Retrieves incident reports filled by citizens through the LexisNexis' Self-Service Citizen report application. They are reports related to property offenses. These reports are reviewed by Records to ensure TIBRS rules are followed.

59.n.19b. Direction: 1-Way Import Citizen incident reports

59.n.19c. Module: Incident

59.n.19d. Format: XML

59.n.19e. Exchange: SFTP

59.n.20. Open Data for Public Website

59.n.20a. Incident, Accident, Calls for Service data daily. Obfuscate address for open cases. There is minimal victim information. Juvenile reports are not shared.

59.n.20b. Direction: 1-Way export

59.n.20c. Module: Incident, Calls for Service, and Accident

59.n.20d. Format: CSV flat files

59.n.20e. Exchange: SFTP

59.n.21. Nashville Mayor's Office Interface

59.n.21a. Daily Incidents and Calls for Service. The address is obfuscated for juvenile and sex crime incidents. The victim information is redacted as well.

59.n.21b. Direction: 1-Way export

59.n.21c. Module: Incident, Calls for Service

59.n.21d. Format: Flat file

59.n.21e. Exchange: SFTP

59.n.22. Jury Search for District Attorney

59.n.22a. District Attorney's office sends a flat file with potential jurors and MNPd runs a report verifying criminal history.

59.n.22b. Direction: Bi-Directional

59.n.22c. Module: Master Name, Court Documents, Arrests?

59.n.22d. Format: Flat file in, PDF out

59.n.22e. Exchange: eMail

59.n.23. Metro Citations (TVIS – Traffic Violations Information System)

59.n.23a. List of moving violations, environmental violations, and parking violations from Traffic Violations Bureau into the RMS Citations module

59.n.23b. Direction: 1-Way import Citations

59.n.23c. Module: Citations

59.n.23d. Format: Oracle SQL Views

59.n.23e. Exchange: Oracle SQL Views

59.n.24. OCA (Persons currently in County Jail)

59.n.24a. Import of Davidson County arrestees currently in jail. The key is the OCA (unique identifier of the person), the retrieve field is the jail location.

59.n.24b. Direction: 1-Way import

59.n.24c. Module: Custom table displayed on Master Name Index module

59.n.24d. Format: Oracle SQL Views

59.n.24e. Exchange: Oracle SQL Views

59.n.25. Mugshot Web Service

59.n.25a. MNPd provides the latest front-view mugshot associated with a person to DCSO and Courts

59.n.25b. Direction: 1-Way export

59.n.25c. Module: Master Name

59.n.25d. Format: Web service call by OCA

59.n.25e. Exchange: Web Service

59.n.26. Inmate Release

59.n.26a. Historical information of people in/has been in DCSO facilities (released or not). It is retrieved by OCA. Currently, we receive information for adults.

59.n.26b. Direction: 1-Way import

59.n.26c. Module: Custom SQL table

59.n.26d. Format: Oracle SQL Views

59.n.26e. Exchange: Oracle SQL Views

59.n.27. Motorola's Body Worn Camera System

59.n.27a. Provide list of recent incidents output to flat file. This is to validate incidents on the Motorola BWC system

59.n.27b. Direction: 1-Way export

59.n.27c. Module: Incidents

59.n.27d. Format: Flat File

59.n.27e. Exchange: File system

59.n.28. Alarm Permits

59.n.28a. Import of Alarm Permits data from Network File System (NFS). The vendor is Citiworks GIS Management.

59.n.28b. Direction: 1-Way import

59.n.28c. Module: Alarm Permits

59.n.28d. Format: Flat file

59.n.28e. Exchange: SFTP

59.n.29. Tennessee Incident Based Reporting (TIBR) Interface

59.n.29a. Provide incident and arrest information to the Tennessee Incident Base Reporting. The data is extracted from RMS in XML format files. It is uploaded to the CrimeInsight website.

59.n.29b. Direction: 1-Way export

59.n.29c. Module: Incident/Arrest

59.n.29d. Format: XML

59.n.29e. Exchange: Drop file on CrimeInsight website

59.n.30. BlueTeam Interface

59.n.30a. Demographic and assignment employee information provided to BlueTeam application.

59.n.30b. Direction: 1-Way export

59.n.30c. Module: Employee

59.n.30d. Format: Oracle SQL Views

59.n.30e. Exchange: Oracle to SQL

59.n.31. MNPD Data Pool

59.n.31a. Accidents, calls for service, arrests, juvenile contacts, citations, warrants, evidence, gang members, incidents, inventory, master names, warrants, etc. provided to Crime Analysis unit internal to MNPD.

59.n.31b. Direction: 1-Way export

59.n.31c. Module: Various

59.n.31d. Format: Views from Oracle to SQL tables

59.n.31e Exchange: Oracle views to SQL tables

59.o.32. Criminal Justice Information Systems (CJIS) Bond Conditions (currently inactive)

59.n.32a. Bond conditions for arrestees through a web service provided by Justice Information Systems.

59.n.32b Direction: 1-Way MNPDP Consume

59.n.32c. Module: N/A

59.n.32d. Format: Oracle SQL Views, PDF

59.n.32e Exchange: Web service

59.n.33. Strategic Development Division Crime Analysis Interface

59.n.33a. Various RMS tables required for internal analysis and reports provided to internal resources

59.n.33b. Direction: 1-Way Export

59.n.33c. Module: Various

59.n.33d. Format: Oracle SQL Views

59.n.33e. Exchange: Oracle views to SQL tables/ SQL to SQL tables

60. RMS – Geographic Information System (GIS)

60.a. Provide Geographic Information System (GIS) Capabilities for the RMS.

60.b. The proposed RMS should include comprehensive GIS capabilities or support seamless integration with industry-standard GIS platforms. These capabilities should enhance situational awareness, crime analysis, resource allocation, and officer safety through geographic data visualization and spatial analysis.

60.c. The Offeror should ensure the proposed RMS solution will leverage GIS functionality to support operational and analytical needs within law enforcement workflows.

60.d. The RMS should support real-time and historical mapping of incident locations, arrests, citations, field interviews, and other relevant records.

60.e. The RMS should support layered map visualization (e.g., incidents overlaid with patrol zones, crime hotspots, and critical infrastructure).

60.f. The RMS should support batch geocoding of records.

60.g. The RMS should notify users of invalid or ambiguous addresses and offer correction tools.

60.h. The RMS should support the generation of crime density maps (heatmaps), trend mapping, and time-series spatial analysis.

60.i. GIS data should be exportable for use in external crime analysis tools (e.g., ArcGIS, QGIS).

60.j. The RMS should support geo-fencing to trigger alerts when events occur within defined areas (e.g., schools, high-crime areas).

60.k. The RMS should support watchlists tied to geographic locations or zones of interest.

60.l. The RMS should natively support or integrate with Esri ArcGIS Server/Online, OpenStreetMap, or similar GIS platforms.

60.m. The RMS should import and export GIS data using standard formats (e.g., shapefiles, GeoJSON, KML, Web Map Service (WMS), Web Feature Service (WFS)).

2.9 Section 9. Equal Business Opportunity (EBO) Program Requirements

1. **EQUAL BUSINESS OPPORTUNITY (EBO) GOAL**

2.

2.10 Section 10. Insurance Requirements

1.

Insurance Requirements

Any offeror receiving an intent to award letter shall be **required** to provide a Certificate of Insurance within **seven (7) calendar days** of receiving the notification in order to proceed with award and execution of a contract.

The Description section must read as follows: **Metropolitan Government of Nashville and Davidson County, its officials, officers, employees, and volunteers are named as additional insureds per general liability additional insured endorsement and automobile liability additional insured endorsement.**

In the Certificate Holder section it must read as follows: **Purchasing Agent, Metropolitan Government of Nashville and Davidson County, Metro Courthouse, Nashville, TN 37201.**

The following insurance(s) shall be required:

2.
 - **General Liability Insurance** in the amount of one million (\$1,000,000.00) dollars per occurrence and in the amount of two million (\$2,000,000) in the aggregate.
3.
 - **Automobile Liability Insurance** in the amount of one million (\$1,000,000.00) dollars combined single limit.
4.
 - **Worker's Compensation Insurance** with statutory limits required by the State of Tennessee or other applicable laws and Employer's Liability Insurance with limits of no less than one hundred thousand (\$100,000.00) dollars, as required by the laws of Tennessee.
5.
 - **Cyber Liability Insurance** in the amount of four million (\$4,000,000.00) dollars.
6.
 - **Technological Errors and Omissions Liability Insurance** in the amount of one million (\$1,000,000.00) dollars.

2.11 Section 11. Standard Solicitation Requirements

1. Pre-Offer Meeting

A pre-offer meeting will be held for this solicitation at **9 am Central Time, Wednesday, June 10, 2026.**

You **must** register in advance to provide the following information: your name, email address, phone number, and the name of the company you are representing by clicking on the following link.

<https://nashville.webex.com/weblink/register/raee82cd7bff6ff7fc36ed785b96c8178>

Event Password: metro

The contact information provided will generate on the Pre-Offer Attendee List if you attend the meeting.

You will receive a confirmation email invitation after you register with the information needed to participate in the Pre-Offer via Webex that will be added to your calendar. You may participate by clicking the Webex Link provided in the email confirmation from a computer, tablet, or smartphone.

If you have any issues with registering for the meeting, please contact the Buyer, **Terri Ray**, terri.ray@nashville.gov, 615-862-6669

Metro urges all prospective offerors to attend planned pre-offer meetings.

Attachments:

File Name or URL	Type	Description
Pre-Offer Attendee Sheet.pdf	File	Amendment #2

2.

Inquiries

All inquiries must be submitted by **Wednesday, June 24, 2026, at 3:30pm Central Time** using the online discussions feature of the iSupplier system. Questions will be answered formally via Amendment to the solicitation soon after the deadline for submitting

questions. Offerors must clearly understand that the only official answer or position of Metro will be the one stated in writing by Division of Procurement staff.

You may contact Terri Ray, terri.ray@nashville.gov or 615/862-6669 with questions regarding iSupplier or you may email iSupplier@nashville.gov (make sure to include your W-9 in email to iSupplier Team). All offerors are encouraged to sign in to the iSupplier system as soon as possible to view the solicitation and ensure all login information is correct.

Finally, please have your offer loaded in the iSupplier system well in advance of the deadline for submission of offers to avoid any last minute functionality issues. While Metro makes every attempt to assist suppliers with entering their offers, there is not sufficient time to trouble shoot functionality issues within one hour of the deadline for submission of offers.

3.

Accurate Information

Failure to provide complete and accurate information in an offer to this solicitation may result in your offer being deemed nonresponsive. Metro may institute debarment proceedings against the offeror and/or terminate any contract or purchase order that has been awarded based on inaccurate information.

Extraneous Information

Offers should be brief and concise. Information provided beyond the requirements described in this solicitation may be considered extraneous and as a result discarded.

Minor Irregularities

Metro reserves the right to waive minor irregularities in offers, provided that such action is in the best interest of Metro. Any such waiver shall not modify any remaining solicitation requirements or excuse the offeror from full compliance with the solicitation specifications and other contract requirements if the offeror is awarded a contract.

Ambiguity, Conflict or Other Errors in the Solicitation

Offeror is responsible for clarifying any ambiguity, conflict, discrepancy, omission, or other error in this solicitation prior to submitting their offer, or it shall be waived. Claims of ambiguity after submission of the offer shall not serve as grounds for a protest.

If an offeror discovers any ambiguity, conflict, discrepancy, omission, or other error in the solicitation, they shall immediately request modification or clarification using the online discussion feature of iSupplier. Required modifications or clarifications will be issued by solicitation amendment.

Validity of Offers

All offers shall be valid for a period of one-hundred and fifty (150) days from the closing date of the solicitation unless another timeframe is agreed to by all parties. Submission of an offer does not afford rights to the offeror nor obligate Metro in any manner.

Offer and Presentation Costs

Metro will not be liable for any costs incurred by an offeror in the preparation of its response to a solicitation, nor for the presentation of its offer and/or participation in any clarifications, discussions, negotiations, or protests.

Rejection of Offers

Metro reserves the right to accept or reject, in whole or in part, any offers submitted. The failure of an offeror to promptly supply information in connection with, or with respect to, reasonable requests may be grounds for a determination of non-responsibility.

Americans with Disabilities Act

Contractor shall ensure Metro that all services provided through this resulting contract shall be completed in full compliance with the 2010 Americans with Disabilities Act (ADA) enacted by law on March 15, 2012 and adopted by Metro. Contractor will ensure that participants at public meetings with disabilities will have communication access that is equally effective as that provided to people without disabilities. Information shall be made available in accessible formats, and auxiliary aids and services shall be provided upon the reasonable request of a qualified person with a disability.

Contractor Personnel Requirements

Subsequent to submission of an offer and prior to award of a contract, key personnel identified in the offer shall not be changed without the approval of Metro. Any changes in key personnel without Metro approval may result in the offer being rejected and not considered for award.

Unauthorized Work

The successful offeror shall not begin work until Metro issues a Notice to Proceed or Purchase Order. Any unauthorized work shall be deemed non-compensable and the offeror will have no recourse against Metro.

***4. Persons Suspended or Debarred from Procurement**

Pursuant to Metro Code 4.36.020, a public list of suspended or debarred persons is maintained by the division of purchases (see link provided herein). Individuals appearing on said list may not be awarded a Metro contract.

Affirmation

Do you or any proposed subcontractors appear on the list of suspended or debarred

persons?

Attachments:

File Name or URL	Type	Description
Suspended or Debarred Persons List	URL	

Target: No, neither I or any of my subcontractors appear on the list of suspended or debarred vendors.

Select one of the following:-

- ☐ a. No, neither I or any of my subcontractors appear on the list of suspended or debarred vendors.
☐ b. Yes, I or one of my subcontractors appear on the list of suspended or debarred vendors and I am non-responsive.

*5.

Subcontractors/Subconsultants

Offeror **must** enter **ALL** subcontractors/subconsultants/suppliers in the Subcontractor/Subconsultant Form (see attachments below) regardless of their ownership and attach back to the submitted response/quote. All proposed subcontractor/subconsultants and/or suppliers must be registered in iSupplier prior to the solicitation deadline. Offeror should identify those subcontractors/subconsultants and/or suppliers that are Small or Service-Disabled Veteran (SBE/SDV) owned, or those that are Minority or Woman owned as appropriate. All known subcontractors/subconsultants and/or suppliers who will perform a portion of this project **must** be listed. If the prime is a Metro approved SBE/SDV, their self-performance participation should be reflected this subcontractor form.

If no subcontractors/subconsultants are being proposed then indicate such on the Subcontractor/Subconsultant Form and attach back to the submitted response/quote.

Failure to attach the Subcontractor/Subconsultant Form to your submitted response/quote may deem your offer non-responsive.

Attachments:

File Name or URL	Type	Description
Blank Subcontractor Form	File	

Target: Subconsultant Form is Attached

Select one of the following:-

- ☐ a. Subconsultant Form is Attached(*Response attachments are required*)
☐ b. No attachment and offer may be deemed non-responsive

***6. Vendor Checklist**

Offeror must complete the vendor checklist (see attached below) and attach completed document back to the submitted response/quote. Information provided on the completed vendor checklist will be used to develop the resulting outcome if issued an intent to award from the solicitation.

Failure to attach the completed Vendor Checklist to your submitted response/quote may deem your offer non-responsive.

Attachments:

File Name or URL	Type	Description
Blank Vendor Checklist	File	

Target: Attached Completed Vendor Checklist

Select one of the following:-

- ☐ a. Attached Completed Vendor Checklist(*Response attachments are required*)
☐ b. No attachment and offer may be deemed non-responsive

2.12 Section 12. Information Security Agreement

- *1. Complete the Metro Information Security Agreement (MISA) Questionnaire attached to this solicitation. Attached the completed Metro Information Security Agreement (MISA) Questionnaire to your quote response. Using the attached MISA-Exhibit Selection Matrix, determine the applicable MISA Terms and Conditions from the MISA-Exhibits (attached herein) based on your company's completed MISA Questionnaire. The determined MISA Terms and Conditions to be included in the resulting contract, if awarded.

Failure to attach your completed MISA Questionnaire may result in your offer being deemed non-responsive.

Offeror must indicate acceptance of the applicable MISA Terms and Conditions. If any exceptions are taken, attach a PDF file to your quote identifying the exceptions and label it as MISA Terms and Conditions Exceptions.

Please note that if exceptions are not stated at this time, they will not be granted after the contract is awarded. Exceptions taken after the award will result in the withdrawal of the intent to award and offeror's firm suspended from upcoming solicitations.

Attachments:

File Name or URL	Type	Description
MISA Terms and ConditionsMISA Exhibit - Terms and Conditions	File	
MISA-Exhibit Selection Matrix	File	
MISA Questionnaire	File	

Target: ISA Questionnaire Completed and Terms and Conditions Accepted

Select one of the following:-

- ☐ a. ISA Questionnaire Completed and Terms and Conditions Accepted (*Response attachments are required*)
☐ b. No, Offer is non-responsive

2.13 Section 13. Solicitation Acceptance

*1.

Offeror must indicate acceptance of the final version of this solicitation as amended. In the likely occurrence that an amendment is issued to the solicitation, you must accept the final amendment for your proposal to be accepted. When an amendment is published you will automatically be notified by the iSupplier system, but you are encouraged to regularly check the solicitation for an amendment. If you have submitted a proposal prior to an amendment, you must resubmit your proposal in response to the amendment to avoid failure to submit or a determination of non-responsiveness. This is required whether your offer is affected by the latest amendment or not.

Any exceptions taken to this solicitation must be submitted through the online discussion feature of the system by the date and time shown for inquiry submittal. If an offeror takes exception to this solicitation after the inquiry submittal date and time, their submission may be deemed nonresponsive.

Target: Yes, Accept Solicitation as Presented

Select one of the following:-

- ☐ a. Yes, Accept Solicitation as Presented
☐ b. No, Offer non-responsive

2.14 Section 14. Contract Acceptance

*1.

Offeror must indicate your acceptance or exceptions to the attached draft contract for this solicitation.

This contract will be the master contract document and any additional documents (i.e. service level agreements, escrow agreements, maintenance agreements, license agreements) will be included as exhibits to the master document. Offerors must submit a word document of all additional exhibits (i.e. service level agreements, escrow agreements, maintenance agreements, license agreements) for Metro's review and consideration in the contract. Failure to do this will be considered as not provide any exceptions as stated below.

If any exceptions are taken, attach a redline word document reflecting the proposed changes as well as

justification or explanation for the proposed change. Your response to this section should indicate if exceptions are taken and you should submit the redlined word document named Contract Exceptions back with your response.

If no exceptions to the contract are stated, they will not be granted after the contract is awarded. Exceptions taken after the award will result in the rescind of the intent to award and offeror may be placed on suspended list.

If exceptions to the contract are stated and requested changes are unacceptable based on Metro's review, this may result in the rejection of the proposal as non-responsive.

Attachments:

File Name or URL	Type	Description
Draft Contract	File	

Target: Accept Contract as Presented and don't have any additional exhibits

Select one of the following:-

- ☐ a. Accept Contract as Presented and don't have any additional exhibits
☐ b. Attached exceptions taken of contract presented(*Response attachments are required*)

2.15 Section 15. Evaluation Criteria

1. Evaluation Criteria Response Formatting

Offeror may use illustrations, diagrams, screenshots and/or other digital, sample material to provide additional clarity. No website or hyperlinks will be accepted for consideration as part of the evaluation criteria proposal response.

All submitted proposals should include the following on every page as a header and/or footer:

- RFQ Number
- RFQ Title
- Proposer Name
- Evaluation Criteria Section Title
- Page Numbers

Each PDF document should be named the Evaluation Criteria Section Title as outlined in the solicitation. Make sure keep evaluation criteria PDF separate and do not combine together.

Metro strongly encourages you to submit question and response together for ease of review by evaluation committee.

NOTE: Cover Pages, Table of Contents, and/or Resumes are excluded from any page limited noted below.

*2.

Experiences and Qualifications (300 Points)

EC.1. Company Profile

EC.1.a. Provide the requested information below for your company and its qualifications to support MNPd's RMS needs. Specifically address the following requirements:

EC.1.a.1. RMS Product Name

EC.1.a.2. RMS Version

EC.1.a.3. Provide company background and number of years in the law enforcement RMS market.

EC.1.a.4. Number of employees dedicated to RMS development and number for RMS support.

EC.1.a.5. Provide number of Active RMS Law Enforcement Customers.

EC.1.a.6. Indicate whether your company originally developed the RMS or acquired it from another organization.

EC.2. Law Enforcement RMS Support Experience

EC.2.a. Provide the requested experience information below for three (3) active RMS project/customers whose size, scope, and complexity to that of the Metropolitan Nashville Police Department (MNPd) or larger. Each RMS support experience project/customer shall specifically address the following requirements:

EC.2.a.1. Law Enforcement Agency Name

EC.2.a.2. Department Size – Total number of sworn officers and support personnel)

EC.2.a.3. Year RMS was implemented

EC.2.a.4. Number of RMS Users

EC.2.a.5. Brief Description of the contract scope

EC.2.a.6. Data Hosting: On-Premises, Cloud, or Hybrid?

EC.2.a.6.1. If Hybrid, please describe the data hosting solution in detail.

EC.3. RMS Implementation Experiences

EC.3.a. The Offeror shall provide detailed information regarding three (3) prior RMS implementations of the vendor's proposed solution, particularly those of similar size, scope, and complexity to that of the Metropolitan Nashville Police Department (MNPd).

At a minimum, the Offeror shall include the following for each RMS Implementation reference:

EC.3.a.1. Law Enforcement Agency Name:

EC.3.a.2. Department Size – Total number of sworn officers and support personnel:

EC.3.a.3. Number of RMS Users:

EC.3.a.4. Staffing Model – Roles and responsibilities of both vendor and client personnel throughout the implementation.

EC.3.a.5. Implementation Project Timeline – Planned versus actual schedule, including key milestones and any delays with explanations. Include Implementation Start Date and duration of the RMS implementation.

EC.3.a.6. Project Overview and Basic Scope – A clear description of the project objectives, major deliverables, implementation approach, and overall scope of work performed.

EC.3.a.7. Change Orders – The number of change orders issued, along with a summary of their

purpose, cost impact, root cause, a description of the scope changes, client-driven changes and any unforeseen requirements.

EC.3.a.8. Initial Contracted Project Cost – The originally contracted cost, including software, services, integrations, and any recurring components.

EC.3.a.9. Final Total Project Cost – The total actual cost upon completion, including a breakdown of any variances from the initial cost.

EC.3.a.10. Data Migration and Conversion Complexity – Description of the approach, level of effort, volume, methodology, processes used, challenges encountered, and overall success. Data Migration was from what RMS?

EC.3.a.11. Hosting: On-Premises, Cloud, or Hybrid?

EC.3.a.11.1. If Hybrid, please describe the hosting solution in detail.

EC.3.a.12. RMS Interfaces – Number established for agency and summary of key system integrations (e.g., CAD, JMS, third-party systems) and any associated complexities.

EC.3.a.13. Duration of RMS Support since implementation.

EC.3.a.14. Current Operational Status - Current Operational Status of the system and whether the referenced client is actively using the RMS solution.

EC.3.a.15. System Performance and Stability Post-Implementation - Provide information on system performance including any major defects or outages within the first two (2) years.

EC.3.b. List any RMS implementations within the last three (3) years that you were contracted to accomplish, that failed to go live or remain active for two (2) years of the go-live date. Include the basic reasons for the implementation not being completed or sustained.

EC.3.c. The Offeror is encouraged to provide quantitative metrics where available (e.g., user adoption rates, system performance improvements, reduction in manual processes) and to highlight any factors that contributed to project success or challenges.

File should be limited to 20 pages attached as a PDF and be named Experiences and Qualifications.

Target: Attached Experience and Qualifications PDF

Select one of the following:-

- ☐ a. Attached Experience and Qualifications PDF(*Response attachments are required*)
- ☐ b. No, and are non-responsive

*3.

RMS Implementation and Support (300 Points)

EC.1 Offeror's Approach to Delivering a Modernized, Sustainable RMS

EC.1.a. Provide the requested information below for how your company and proposed RMS solution will support MNPd's current and future operational needs. Specifically address the following requirements:

EC.1.a.1. How will Offeror handle change requests prompted by updates to local, state, or federal laws?

EC.1.a.2. How will Offeror handle change requests prompted by NIBRS/TIBRS code requirements.

EC.1.a.3. Describe Offeror's process for responding to internal MNPd requests that are essential to effective records management.

EC.1.a.4. Describe Offeror's disaster recovery and business continuity plans, including Recovery Time Objective (RTO) – duration of acceptable downtime metrics, Recovery Point Objective (RPO) – amount of acceptable data loss metrics, and Mean Time to Recovery (MTTR) – the average time required to restore the RMS and services to normal operations following an incident.

EC.1.a.5. Provide Offeror's RMS product roadmap for the next 12–24 months.

EC.1.a.6. Provide your perspective on emerging technologies (e.g., Artificial Intelligence, Machine Learning, or other transformative solutions) and how these are integrated into your RMS roadmap.

EC.1.a.7. If MNPD were to establish a long-term partnership with your company, describe where you envision your RMS solution leading us during the life of the contract. Discuss RMS extensibility, scalability, and your approach to meeting MNPD's evolving requirements.

EC.2. RMS – Project Communication Plan

EC.2.a. Provide a Project Communication Plan that demonstrates the capability to provide transparent, timely, and coordinated communications. Specifically address the following;

EC.2.a.1. Outline the primary goals of your communication strategy during the implementation lifecycle.

EC.2.a.2. Outline the structured framework for escalating critical issues, risks, or delays.

EC.2.a.3. Outline how communication will support the submission, review, and approval of change requests, and decision tracking.

EC.2.a.4. Provide stakeholder communication strategies tailored to influence responsibilities, and preferred communication methods. Describe how communication-related roles and responsibilities are clearly defined across the project.

EC.2.a.5. Describe your approach for communicating software release notes and product updates throughout the life of the contract.

EC.2.a.6. Provide a proposed communication structure for meetings cadence, standard reporting formats, and the schedule for delivering project reports.

EC.3. RMS - Project Management Methodology

EC.3.a. Describe the project management methodology including project management techniques which should outline the standard and practices as well as software that will be utilized.

EC.3.b. Describe your approach to managing this project, its tasks and deliverables. The proposed approach should provide for insight into the Offeror's capability to manage the project, respond to day-to-day problems, manage issues, provide regular status reports, coordinate staff, manage project resources, project documentation, and configuration control.

EC.3.c. Demonstrate knowledge of the project objectives, goals, existing conditions and assumptions. Identify potential issues or challenges, your approach to minimizing any disruptions to performance, and present a plan for completing

the specified work in accordance with the scope.

EC.3.d. Describe what process controls will be put in place to ensure the work required throughout this project is performed in a timely and accurate manner.

EC.4. RMS - Implementation Plan

EC.4.a. Provide a Project Implementation Plan, go-live implementation strategies, and roll out plan, for the proposed Records Management System (RMS) that aligns with the solicitation.

EC.4.b. Provide an estimated timeline for the implementation, including milestones, key deliverables, and duration of each project phase (e.g., planning, configuration, testing, training, deployment, post-go-live support). Indicate any dependencies and critical path elements.

EC.4.c. Provide proposed Data Migration plan to ensure a successful migration of data into the proposed RMS.

EC.4.d. Describe how you plan to work with MNPd to develop a detailed statement of work, including an estimate of the time and MNPd resources that would be required to develop and approve the statement of work.

EC.4.d.1. Describe the process by which the system requirements will be validated and incorporated into the statement of work.

EC.4.d.2. Provide a sample statement of work.

EC. 5. RMS - Training Plan

EC.5.a. Provide a comprehensive Training Plan for the proposed RMS implementation that addresses the diverse training needs of the end users and user groups.

EC.5.b. Describe any antecedents/preparatory materials (e.g., orientation videos, RMS overviews, documentation) that will support early user familiarity and help establish a baseline understanding of the RMS before formal training begins.

EC.5.c. Describe all formats in which all reference and training medium will be made available.

EC.5.C.1. Include an overview of your Instructor-Led Training (ILT) if such an approach to training is available for MNPd.

EC.5.d. Outline any continuous learning opportunities via a learning portal, sandbox or testing environment access.

EC.5.e. Provide details regarding formative assessments (during learning) and/or summative assessments (after learning) testing materials relevant to individual training classes to help ensure transfer of knowledge to the students. Describe how the transfer of knowledge is effectively measured.

EC.5.f. In the event an upgrade impacts any component of the RMS, what is the training plan for the user level(s) impacted by the change?

EC.6. RMS- Customer Service and Support Plan

EC.6.a. Demonstrate a well-defined and measurable customer service philosophy supported by industry best practices and validated performance metrics (e.g., MTTR, CSAT, NPS).

EC.6.b. Explain the structure, and effectiveness of the proposed tiered support framework, including issue classification, escalation procedures, response times, availability, and support channels.

EC.6.c. Provide details on the approach to providing ongoing customer and technical support, including training, helpdesk operations, account management, and proactive support activities.

EC.6.d. Explain the adequacy and reliability of risk management and disaster recovery/business continuity planning,

and how they will ensure uninterrupted service delivery and rapid recovery from system disruptions.

EC.7. RMS- Quality Plan

EC.7.a. Describe how the extent to which the Offeror's Quality Plan demonstrates a comprehensive and integrated approach to ensuring accuracy, integrity, compliance, performance, user satisfaction, and security across the full RMS lifecycle.

EC.7.b. Demonstrate the degree to which the proposed Quality Plan aligns with and ensures adherence to applicable standards, including CJIS, NIBRS/TIBRS, ANSI/NIST, and all relevant federal, state, and MNPd requirements.

EC.7.c. Describe the completeness and rigor of the risk, issue, and change management processes and supporting documentation as they relate to maintaining quality throughout implementation and ongoing operations.

EC.7.d. Describe the thoroughness and appropriateness of the proposed testing strategy, data migration validation procedures, quality metrics, and reporting mechanisms to ensure system reliability, accuracy, and performance.

EC.7.e. Describe the strength of the approach to quality control during deployment, training, and ongoing maintenance, including monitoring, continuous improvement, compliance reviews, and defined service levels.

File should be limited to 50 pages attached as a PDF and named RMS Implementation and Support.

Target: AttachedRMS Implementation and Support PDF

Select one of the following:-

- ☐ a. AttachedRMS Implementation and Support PDF(*Response attachments are required*)
- ☐ b. No, and are non-responsive

*4.

RMS Technical Overview (700 Points)

EC.1 RMS Graphical User Interface (GUI)

EC.1.a. Provide five (5) RMS screen captures of the proposed Records Management System (RMS). These five (5) screen captures should contain one (1) opening screen or landing page, and four (4) other random screen captures that highlight your RMS. These screen captures will be evaluated for their clarity, logical menu workflow and other aesthetic features that support a professional and pleasing GUI environment.

EC.1.b. Provide a comprehensive and detailed menu tree (hierarchical flow chart) of the proposed Records Management System (RMS). This menu tree must accurately reflect the current production version of the RMS software and include all available menu options, sub-menus, and drop-down selections available to RMS users. The menu tree will be evaluated for logical menu workflow that supports a professional and pleasing GUI environment.

EC.2. RMS — Data Cleansing and Merge Capabilities

EC.2.a. Describe the extent to which the proposed RMS provides accurate and comprehensive duplicate detection and data cleansing across all required data domains.

EC.2.b. Describe the degree to which the solution supports configurable and effective matching criteria, including exact, fuzzy, and multi-field matching.

EC.2.c. Describe the extent to which authorized users can review, validate, and perform controlled record merges while preserving data relationships and integrity. Additionally, describe the system's ability and defined process for backing out of any controlled record merge, including restoration of pre-merge data states, preservation of audit trails, and assurance that data integrity and relationships remain fully intact.

EC.2.d. Describe the completeness of audit trails and the system's ability to maintain data integrity, reporting accuracy, and evidentiary chain of custody.

EC.2.e. Describe the quality of reporting, dashboards, administrative controls, and any AI/ML capabilities that enhance data cleansing and merging management.

EC.3. RMS - Interface Connectivity

EC.3.a. Demonstrate your capability and provide a comprehensive plan for establishing the connectivity of all existing system interfaces from the current Records Management System (RMS) to the proposed RMS solution. The migration plan shall address the approach, methodology, tools, and resources that will be used to ensure continuity of data exchange and operational functionality during and after the transition.

EC.3.b. Disclose any licensing, development toolkits, or middleware required for future integrations.

EC.3.c. For each of the thirty-four (34) integrations Metro currently requires, please provide a response for the following questions:

EC.3.c.1. Is this interface as described in your base product?

EC.3.c.2. If not, have you developed this interface for customers before? For how many customers have you developed and supported this interface?

EC.3.c.3. Provide scope of the interface you developed including, at a minimum, data direction, data formats, data exchange methods:

EC.3.c.4. Provide details on any other available data exchange methods that would be available to us for this interface. Describe security, efficiency, and performance advantages for these available data exchange methods. that would be available to us for this interface:

EC.3.c.5. Provide details on how the health/status of the interface is effectively monitored and audited within your platform.

EC.4. RMS-MNPD Field Reporting

EC.4.a. The Offeror should refer to the MNPD RFP RMS Field Report PDFs_v.2026 attachment to this RFP. Each one of the twenty-three (23) MNPD Field Reports presented in the MNPD RFP RMS Field Report PDFs_v.2026 needs to be available to our police officers both in office and when working remotely. Examine each Field Report and explain how your proposed RMS provides for: (1) form submission from the field, (2) the capture of ALL fields in the form, (3) and state if all fields listed will be available to MNPD in the RMS.

EC.4.b. Any exceptions or compromises must be noted.

EC.4.c. Further, describe any limitations to additional customizable fields available for each report.

EC.4.d. Describe the processes required to edit an existing report, and to create a new report.

EC.4.e. Provide relevant Field Reporting documentation and user guides for the proposed RMS.

EC.5. RMS — Geographic Information System (GIS) Capabilities

EC.5.a. Describe how your proposed RMS will support MNPd's Geographic Information System (GIS) capabilities. Include several detailed use cases that demonstrate how users would utilize your RMS.

EC.5.b. Describe how the RMS will leverage GIS functionality to support operational and analytical needs within law enforcement workflows.

EC.5.c. Specify any proprietary GIS requirements or limitations.

EC.5.d. Provide use cases specific to law enforcement, including, but not limited to:

EC.5.d.1. Geographic allocation of patrol resources

EC.5.d.2. Investigation support through spatial data analysis

EC.6. RMS Data Hosting Platform

EC.6.a. Describe all available hosting models (cloud, on-premises, hybrid).

EC.6.b. Provide a complete list of hardware requirements for each proposed deployment model.

EC.6.c. Provide a complete list of all required third-party software components.

EC.6.d. List the details regarding cloud deployment architecture, including:

EC.6.d.1. Number and geographic distribution of data centers

EC.6.d.2. Whether all data centers reside within the United States

EC.6.d.3. FedRAMP authorization status (if applicable)

EC.6.d.4. Disaster recovery capabilities

EC.6.e. Provide documentation demonstrating CJIS compliance.

EC.6.f. Provide information describing system scalability, including:

EC.6.f.1. Ability to support increasing users and sites

EC.6.f.2. Horizontal vs. vertical scaling approach

EC.6.f.3. Performance under peak conditions

EC.6.g. Describe monitoring, alerting, and system management capabilities.

EC.6.h. Provide confirmation that MNPd will incur no limitations or additional fees for accessing or extracting agency-owned data to an on-premise data lake or other third-party systems used by MNPd.

EC.7. RMS — Data Quality Attributes

EC.7.a. Describe the extent to which the RMS ensures accuracy, consistency, completeness, and reliability of data across all modules.

EC.7.b. Describe the degree to which the solution supports compliance with CJIS, NIEM, NIBRS/TIBRS/UCR, and other applicable standards and regulations.

EC.7.c. Describe the ability of the RMS to scale effectively to accommodate increases in users, transactions, and data volume without degradation in performance.

EC.7.d. Describe the capability of the system to provide consistent, responsive performance and high availability under normal and peak operational conditions.

EC.7.e. Describe the effectiveness of the RMS in integrating with internal and external systems through APIs, standard data formats, and third-party interfaces.

EC.7.f. Describe the extent to which the solution provides tools, environments, and processes for efficient system testing, validation, and automated quality assurance.

EC.7.g. Describe the degree to which the system supports efficient maintenance with minimal down-time, including modular architecture, ease of updates and patches, and vendor support for enhancements.

EC.7.h. Describe the ability of the RMS to provide seamless access across desktop, web, and mobile platforms, including support for both cloud and on-premises environments.

EC.7.i. Describe the capability to transfer and manage data across different environments without loss of integrity or functionality.

EC.7.j. Describe the extent to which the RMS supports comprehensive auditing, traceability, and data governance to ensure accountability and transparency.

File should be limited to 90 pages attached as a PDF and be named RMS Technical Overview.

Target: Attached RMS Technical Overview PDF

Select one of the following:-

- ☐ a. Attached RMS Technical Overview PDF(*Response attachments are required*)
- ☐ b. No, and are non-responsive

*5.

RMS Modules (700 Points)

EC.1. RMS Module Narrative

EC.1.a. For each module or system component listed in the RFP Scope, provide a narrative including, but not limited to:

EC.1.a.1. Is this module included in your base RMS solution?

EC.1.a.1a. If not, describe what is required for integration.

EC.1.a.2. Identification of any system limitations, or optional features.

EC.1.a.3. Description of workflow configuration options, including routing, approvals, supervisory review capabilities, and associated audit trail functionality.

EC.1.a.4. Description of search, reporting, analytics, and data export capabilities available within the module.

EC.1.a.5. Description of mobile functionality, including support for field-based access, offline operation, and synchronization processes.

EC.1.a.6. Description of security controls, including role-based access permissions, CJIS compliance, and data retention configuration capabilities.

EC.1.b. For each functional requirement listed within the module or system component, clearly indicate the level of compliance using one of the following designations:

EC.1.b.1. Offeror should refer to each requirement by "number" outlined in the scope details for easy reference.

EC.1.b.1a. **Fully Comply (YES)** – The requirement is fully satisfied through standard system functionality.

EC.1.b.1b. **Partially Comply (PC)** – The requirement is partially satisfied and may require additional configuration, customization, or third-party integration. Provide details.

EC.1.b.1c. **Requirement not Supported (NO)** – The requirement is not supported by the proposed solution.

EC.1.b.1d. For any requirement that is not rated as "Yes", meaning the functionality cannot be met with the current system that is in production elsewhere, the Offeror should provide an explanation for that requirement's rating.

EC.1.c. MNPD is currently using BOLO module for Warrant Deconfliction; does your firm offer a different way of handling Warrant Deconfliction when multiple officers attempt to serve warrants on the same day?

EC.1.d. Provide a list of all modules available in your RMS (in addition to the above). Note whether they come standard within the RMS product, or if they are ancillary and available by other means.

EC. 2. RMS-Crime Analytics Module: Additional Module Evaluation Criteria

EC. 2.a. Provide ten (10) examples of reports generated by your RMS, including, a variety of operational and supervisory reports and at least five (5) examples of Community Engagement Reports appropriate for public posting.

EC.3. RMS- Court Document for Adults Module: Additional Module Evaluation Criteria

EC.3.a. Describe how the proposed RMS will support MNPd's warrant deconfliction processes, including the ability to track warrant service activities, identify and flag conflicts, and manage deconfliction workflows when multiple enforcement units are involved. The response shall outline how the system records, monitors, and alerts personnel to overlapping operations or service attempts and how authorized users may view, update, and coordinate deconfliction status within the RMS.

EC.4. RMS Master Indices Modules

EC.4.a. Provide details on the Comprehensiveness and Structure of Master Indices which should include the following:

EC.4.a.1. The extent to which the proposed RMS provides centralized, fully integrated Master Indices across all required entity types with unique identifiers and robust linkage of associated records.

EC.4.b. Provide details on Data Quality, De-duplication, and Identity Resolution.

EC.4.b.1. The effectiveness of the solution's data validation, duplicate prevention, configurable merge rules, and AI-driven identity resolution capabilities, including accuracy, confidence scoring, and continuous learning.

EC.4.c. Provide details on Search, Usability, and Data Relationships

EC.4.c.1. The ability of the RMS to deliver advanced, high-performance search capabilities, intuitive navigation, comprehensive profile views, and visual relationship mapping across all Master Index records.

EC.4.d. Provide details on Security, Access Control, and Auditability

EC.4.d.1. The degree to which the system enforces role-based access, protects sensitive data, and provides complete audit trails for all access, changes, and record management activities.

EC.4.e. Provide details on Interoperability, Performance, and Data Migration

EC.4.e.1. The capability of the RMS to integrate with internal and external systems using standard formats and APIs, support scalable performance, and ensure accurate, efficient migration and transformation of legacy Master Index data.

EC.4.f. Offerors shall provide detailed descriptions of each of the five (5) Master Index modules as well as the following information for each:

EC.4.f.1. Configuration options and administrative controls.

EC.4.f.2. Duplicate detection and merge functionality details.

EC.4.f.3. Relationship mapping capabilities.

EC.4.f.4. Search performance metrics.

EC.4.f.5. Security and CJIS compliance documentation.

EC.4.f.6. Integration architecture documentation.

54.h.5.h. Provide in detail information about data migration approach for legacy index records.

54.h.5.i. Provide in detail information for reporting and analytics capabilities.

54.h.5.k. Provide in detail information about Identification of all standard functionality versus custom development required to meet these requirements.

File should be limited to 100 pages attached as a PDF and be named RMS Modules.

Attachments:

File Name or URL	Type	Description
Economic Engagement Assessment	File	

Target: Attached RMS Modules PDF

Select one of the following:-

- ☐ a. Attached RMS Modules PDF (Response attachments are required)
- ☐ b. No, and are non-responsive

2.16 Section 16. Affidavits

*1.

Compliance with Laws: After first being duly sworn according to law, the undersigned (Affiant) states that he/she and the contracting organization is presently in compliance with, and will continue to maintain compliance with, all applicable federal, state, and local laws.

Taxes and Licensure: Affiant states that Contractor has all applicable licenses, including business licenses. Affiant also states that Contractor is current on its payment of all applicable gross receipt taxes and personal property taxes. M.C.L. 4.20.065.

Nondiscrimination: Affiant affirms that by its employment policy, standards and practices, it does not subscribe to any personnel policy which permits or allows for the promotion, demotion, employment, dismissal or laying off of any individual due to race, creed, color, national origin, age or sex, and are not in violation of, and will not violate, any applicable laws concerning the employment of individuals with disabilities. M.C.L. Section 4.28.020.

Covenant of Nondiscrimination: Affiant affirms that in consideration of the privilege to submit offers in response to this solicitation, we hereby consent, covenant, and agree as follows:

- To adopt the policies of the Metropolitan Government relating to equal opportunity in contracting on projects and contracts funded, in whole or in part, with funds of the Metropolitan Government;
- To attempt certain good faith efforts to solicit Minority-owned and Woman-owned business participation on projects and contracts in addition to regular and customary solicitation efforts;
- Not to otherwise engage in discriminatory conduct;
- To provide a discrimination-free working environment;
- That the Covenant of Nondiscrimination is requirement to submit an offer and shall be incorporated by reference into any contract or portion thereof which the Supplier may hereafter obtain; and shall be continuing in nature and shall remain in full force and effect without interruption.
- That the failure of the Supplier to satisfactorily discharge any of the promises of nondiscrimination as made and set forth herein shall constitute a material breach of contract. M.C.L. Section 4.46.070.

Affiant affirms that in consideration of the privilege to submit offers in response to this solicitation, we hereby consent, covenant, and agree as follows:

1. No person shall be excluded from participation in, denied the benefit of, or otherwise discriminated against on the basis of race, color, national origin, gender, or disability when otherwise qualified in connection with any solicitation offer submitted to Metro or the performance of any contract resulting from;
2. That it is and shall be the policy of this Company to provide equal opportunity to all business persons seeking to contact or otherwise interested in contracting with this Company, including various eligible business enterprises;
3. In connection herewith, I/We acknowledge and warrant that this Company has been made aware of, understands and agrees to make good faith efforts to solicit disadvantaged businesses (as defined in M.C. L. Section 4.46) to do business with this Company;
4. That the Covenant of Nondiscrimination as made and set forth herein shall be continuing in nature and shall remain in full force and effect without interruption;
5. That the Covenant of Nondiscrimination as made and set forth herein shall be and are hereby deemed to be made a part of, and incorporated by reference into, any contract or portion thereof which this Company may hereafter obtain; and
6. That the failure of this Company to satisfactorily discharge any of the Covenant of Nondiscrimination as made and set forth herein shall constitute a material breach of contract entitling Metro to declare the contract in default and to exercise any and all applicable rights and remedies, including but not limited to, termination of the contract, suspension and debarment from future contracting opportunities, and withholding and/or forfeiture of compensation due on a contract.

Should you decline this covenant, your firm/organization will not be allowed to submit an offer to the Metropolitan Government of Nashville and Davidson County.

Employment Requirement: Affiant affirms that Contractor's employment practices are in compliance with applicable United States immigrations laws. M.C.L. Section 4.40.060.

Contingent or Brokerage Fees: It is a breach of ethical standards for a person to be retained, or to retain a person, to solicit or secure a Metro contract upon an agreement or understanding for a contingent commission, percentage, or brokerage fee, except for retention of bona fide employees or bona fide established commercial selling agencies for the purpose of securing business. After first being duly sworn according to law, the undersigned Affiant states that the Offeror has not retained anyone in violation of the foregoing. M.C.L. Section 4.48.080.

Iran Divestment Act: By submission of this offer and in response to the solicitation, offeror(s) and each person signing on behalf of offeror(s) affirm, under penalty of perjury, that to the best of their knowledge and belief, neither the offeror(s), nor proposed subcontractors, subconsultants, partners and any joint venturers, are on the list created pursuant to the Tennessee Code Annotated Section 12-12-106 (Iran Divestment Act). Referenced website reflected in the attachment section herein.

Sexual Harassment: Affiant affirms that should it be awarded a contract with the Metropolitan Government for a period of more than twelve (12) months and/or valued at over five hundred thousand (\$500,000) dollars, affiant shall be required to provide sexual harassment awareness and prevention training to its employees if those employees:

- Have direct interactions with employees of the Metropolitan Government through email, phone, or in-person contact on a regular basis;
- Have contact with the public such that the public may believe the contractor is an employee of the Metropolitan Government, including but not limited to a contractor with a phone number or email address associated with Metropolitan government or contractors with uniforms or vehicles bearing insignia of the Metropolitan Government; or
- Work on property owned by the metropolitan government.

Such training shall be provided no later than (90) days of the effective date of the contract or (90) days of the employee's start date of employment with affiant if said employment occurs after the effective date of the contract. M. C.L. Section 2.230.020.

Boycott of Israel: Affiant affirms that Contractor is not currently, and will not for the duration of the awarded Contract, engage in a boycott of Israel for any awarded contract that meets the following criteria:

- Has total potential value of two hundred fifty thousand (\$250,000) or more;
- Affiant has ten (10) or more employees.

Procurement Code: Affiant affirms that offeror is and will remain in compliance with the provisions of Chapter 4.12 of the Metro Procurement Code and the contents of its offer as submitted. Affiant further affirms that offeror understands that failure to remain in such compliance shall constitute a material breach of its agreement with the Metropolitan Government.

Attachments:

File Name or URL	Type	Description
Iran Divestment Act	URL	

Target: Yes, I so affirm to ALL Affidavits

Select one of the following:-

- ☐ a. Yes, I so affirm to ALL Affidavits
- ☐ b. No, and are non-responsive

2. And Further Affiant Sayeth Not:

*3. Name of Company Officer and Title:

Target: Company Officer Name, Title

*4. Enter City, County, State, and Zip Code for Company Location

Target: City, County, State, Zip Code

*5. The provision of false information is a material breach.

Target: Acknowledge and Understand

Select one of the following:-

- ☐ a. Acknowledge and Understand
- ☐ b. Do not acknowledge and/or understand, Offer is non-responsive

6. *If the principal officer cannot so attest, the offer will be determined non-responsive.*

3 Contract Terms

Contract Terms and Conditions

GG Standard PO Terms and Conditions

GG Standard Purchase Order Terms and Conditions

The following terms and conditions are non-negotiable for PO's originating from departmental quotes and PO's issued in response to Invitations to Bid (ITB) or Requests for Proposals (RFP) where no formal contract was developed. If the PO is issued as a release against a filed contract, the contract's terms and conditions shall govern. Otherwise, the submission of a bid or proposal is a formal acceptance by Supplier of Metro's Terms and Conditions.

1. **GENERAL:** The terms and conditions of this PO must not be changed by Supplier. If the PO, in response to the solicitation, is not acceptable, return the PO to Metro's Procurement Division. Failure to deliver or to comply with any of the terms and conditions of this PO or any contract upon which this purchase order is based, may disqualify Supplier, and may result in the cancellation of this PO, solicitation or contract and damages being charged to the Supplier. Suspension and Debarment may also be determined by the Purchasing Agent to be warranted.
2. **QUALITY:** All goods or services furnished pursuant to this PO must be specified, and subject to the approval and inspection of Metro within a reasonable time after delivery at destination. Variations in goods or services from those specified in this PO must not be made without written authority from the Purchasing Agent. Goods rejected will be returned at Supplier's risk and expense.
3. **QUANTITY PRICE:** The quantity of goods or services ordered or the price specified must not be exceeded without authority from the Purchasing Agent. No industry standard of 'plus or minus X%' will be honored unless permitted in the solicitation and the offer in response to the Metro solicitation.
4. **PACKAGING:** Damage to any goods received will result in rejection of the shipment. The goods will not be returned unless supplier assumes return shipment expenses. Packages must be marked plainly with shipper's name and appropriate PO number. No charges shall be allowed for boxing or crating unless previously agreed upon in writing.
5. **DELIVERY:** All goods must be shipped F.O.B. Destination, Freight Prepaid by Seller, Inside Delivery unless otherwise specified in the response offer to the Metro solicitation, contract or this PO. Supplier assumes all risks and responsibility for freight charges, bears the freight expense, owns the goods in transit, and files transportation claims if warranted. Metro will pay no freight or expense charges except by previous agreement in writing. Deliveries must be affected within the time stated on the solicitation, contract or purchase order. Deliveries shall be made between 8 a.m. and 4 p.m. Monday through Friday unless otherwise stated in the solicitation, contract or PO. In case of default by Supplier, Metro may procure the goods or services covered by this PO from other sources and hold Supplier responsible for any excess expense incurred.
6. **PAYMENT:** All payments are made by established ACH. To ensure timely receipt of payment, clearly reference the PO number on the invoice. Only one PO number may be referenced on an invoice. If there are multiple shipments or multiple milestone payments on a PO, there may be multiple invoices referencing the same PO number.
7. **PROPER INVOICE:** For an invoice to be a proper invoice, the requirements shall be set forth in the contract governing the purchase; however, no invoice submitted by Supplier shall be considered a proper invoice unless the invoice is an original invoice, is delivered to Metro in accordance with the PO, correlates to the PO under which the purchase was made, and sets forth the following additional information:
 - The Name of the business organization that is cited in Metro's PO;
 - The Date of the PO preparation;
 - Identifying invoice number;
 - Supplier's federal identification number;
 - Description of the goods, services, or property provided to Metro;
 - Metro's part or item number for each item or part delivered;
 - Delivery terms stated on Metro's PO;
 - Location and date of delivery of the goods, services, or property to Metro;

- Quantity of the goods, services, or property provided to Metro referencing the same unit of measure as Metro's PO;
 - Unit price of the goods, services, or property provided to Metro matching the unit price on Metro's PO;
 - Additional shipping costs or fuel surcharges if permitted in the solicitation, provided in the bid response, and included in the line descriptions of the PO.
 - Extended total price of the goods, services, or property provided to Metro based on the PO unit(s) of measure; and
 - Applicable discounts.
8. **SUPPLIER SELF-SERVICE:** Supplier self-service is provided for the ACH payments. It is the Supplier's responsibility to access Metro's supplier self-service website.
 9. **ASSIGNMENT:** Supplier shall not assign, transfer, convey or otherwise dispose of the PO, or the right, title or interest in or to the same of any part thereof, without the prior written consent of Metro, and Supplier shall not assign by power of attorney or otherwise any of the moneys to become due and payable under the PO. Breach of this provision shall be a material breach.
 10. **CONTINUOUS SUPPLY:** It is understood that it is necessary for Metro to have a continuous and uninterrupted flow of supplies and materials and Supplier must furnish and make the deliveries accordingly.
 11. **LEGAL COMPLIANCE:** The PO is subject to all Charter and Code provisions of Metro. It is hereby agreed that the provisions of all ordinances and resolutions of Metro relating to Suppliers are hereby made a part of the PO.
 12. **CANCELLATION:** Should Supplier fail to fulfill, in a timely and proper manner, its obligations under the PO, or if it should violate any of the terms of the PO, Metro shall have the right to immediately cancel the PO. Metro may cancel the PO at any time, with or without cause, upon sixty (60) days' written notice to Supplier. Should funding for the PO be discontinued, Metro shall have the right to cancel the PO.
 13. **POSSIBLE CURE:** Metro, at its option, and in lieu of immediate cancellation, may request that Supplier repair or replace any defective goods by written notice to Supplier. In that event, Supplier shall repair or replace the defective good(s) within thirty (30) days. Exercise of this option shall not relieve Supplier of any liability to Metro for damages sustained by virtue of Supplier's breach.
 14. **PO CHANGE:** The PO may be modified only by PO change amendment executed by all parties. All change orders, where required, shall be executed in accordance with '4.24.020 of the Metropolitan Code of Laws.
 15. **REMEDY:** No waiver of any provision of the PO shall affect the right of any party thereafter to enforce such revision of to exercise any right or remedy available to it in the event of any other default.
 16. **ATTORNEY FEES:** Supplier agrees that, in the event either party deems it necessary to take legal action to enforce all provisions of the PO, and in the event Metro prevails, Supplier shall pay all expenses of such action including Metro's attorney fees, expert fees, and costs at all stages of the legal action.
 17. **ENTIRE PO:** The PO sets forth the entire agreement between the parties with respect to the subject matter hereof and shall govern the respective duties and obligations of the parties unless the PO is a release against an existing contract, in which case the Contract Terms and Conditions shall prevail.
 18. **GOVERNING LAW:** The validity, construction, and effect of the PO, and any and all extensions and/or modifications thereof shall be governed by the Laws of the State of Tennessee. Any action between the Parties arising from this Contract shall be filed, maintained, and resolved in the Circuit or Chancery Courts of Davidson County, Tennessee. Supplier explicitly waives its right to remove any actions filed in the courts of Davidson County, Tennessee, to Federal court.
 19. **SEVERABILITY:** Should any provision of the PO be declared to be invalid by any court of competent jurisdiction, such provision shall be severed and shall not affect the validity of the remaining provisions of the PO.
 20. **ANTI-TRUST:** Supplier, in determining the prices and/or amounts of this PO, shall not collude with any other person, firm, corporation, or association in arriving at said prices and/or amounts or in any way violate the terms, conditions, and/or spirit of the provisions of 15 U.S.C. 1 through 7 (Sherman Anti-Trust Act).
 21. **ADMINISTRATIVE RIGHTS:** Supplier is entitled to protest to the Purchasing Agent if it is aggrieved in connection with the solicitation or award of a PO. Metropolitan Code of Law (M.C.L.) "4.36.010. Supplier also has the right to appeal the decision of the Purchasing Agent to the Procurement Appeals Board. M.C.L. "4.36.110. This appeal must be filed within seven (7) days of receipt of the Purchasing Agent's decision. M.C.L. "4.36.120.
 22. **SUSPENSION &/or DEBARMENT:** Supplier may appeal the decision of the Purchasing Agent to debar or suspend Supplier from consideration for award of POs or contracts. Metropolitan Code section(s) 4.36.120. This appeal must be filed within thirty (30) days of receipt of the Purchasing Agent's decision.
 23. **INDEMNIFICATION:** Supplier agrees to indemnify and hold the Metropolitan Government, its officers, agents,

and/or employees harmless from and against any and all lawsuits, damages, and expenses, including court costs, expert fees, and attorney's fees, by reason of any claim and/or liability imposed, claimed, and/or threatened against the Metropolitan Government, its officials, agents, and/or employees for damages because of bodily injury, death, and/or property damages arising out of or in consequence of this purchase order to the extent that such bodily injuries, death, and/or property damages are attributable to the acts or omissions of the Supplier and/or the Supplier's officers, agents, and/or employees.

24. **AFFIRMATIONS:** Supplier, by accepting and honoring this purchase order, makes the following affirmative declaration and statement as of the date said purchase order is honored, to wit:
- **Taxes and Licensure.** Supplier states that Supplier has all applicable licenses, including business licenses. Affiant states that Supplier is current on its payment of all applicable gross receipt taxes and personal property taxes. M.C.L. '4.20.065.
 - **Nondiscrimination.** Supplier affirms that by its employment policy, standards and practices, it does not subscribe to any personnel policy which permits or allows for the promotion, demotion, employment, dismissal or laying off of any individual due to race, creed, color, national origin, age or sex, and are not in violation of, and will not violate, any applicable laws concerning the employment of individuals with disabilities. With regard to all aspects of this PO, Supplier certifies and warrants it will comply with this policy. M.C.L. '4.28.020.
 - **Employment Requirement.** Supplier declares that neither the prime, subcontractors, sub-consultants, nor providers of day laborers, employ any person who is not a legal resident of the United States. Any contractor who knowingly violates the provisions of this section is subject to debarment or suspension. M.C.L. 4.40.060.
 - **Contingent Fees.** It is a breach of ethical standards for a person to be retained, or to retain a person, to solicit or secure a Metro contract upon an agreement or understanding for a contingent commission, percentage, or brokerage fee, except for retention of bona fide employees or bona fide established commercial selling agencies for the purpose of securing business. The Supplier affirms that they have not retained anyone in violation of the foregoing. M.C.L. '4.48.080.
25. **IRAN DIVESTMENT ACT:** In accordance with the Iran Divestment Act, Tennessee Code Annotated ' 12-12-101 et seq., CONTRACTOR certifies that to the best of its knowledge and belief, neither CONTRACTOR nor any of its subcontractors are on the list created pursuant to Tennessee Code Annotated ' 12-12-106. Misrepresentation may result in civil and criminal sanctions, including contract termination, debarment, or suspension from being a contractor or subcontractor under METRO contracts.
26. **ISRAEL ANTI-BOYCOTT ACT.** In accordance with Tennessee Code Annotated Title 12, Chapter 4, Part 1 CONTRACTOR certifies that CONTRACTOR is not currently engaged in, and will not for the duration of this Contract engage in, a boycott of Israel.