

LAW ENFORCEMENT mDL TECHNOLOGY TOOLKIT

Portfolio Overview & Guide to the Document Series

ISO/IEC 18013-5 Compliant Mobile Driver License Adoption for Law Enforcement

Prepared by	American Association of Motor Vehicle Administrators (AAMVA)
Version	1.0 April 2026
Standard	ISO/IEC 18013-5 (In-Person mDL) ISO/IEC 18013-7 (Online mDL)

Table of Contents

Portfolio Overview & Guide to the Document Series	1
About This Toolkit.....	4
Background: The mDL Landscape for Law Enforcement	6
Key Contacts & Resources.....	7
Standards Overview.....	9
What Is an mDL?	10
ISO/IEC 18013-5: The In-Person mDL Standard	10
ISO/IEC 18013-7: Online mDL Verification	11
AAMVA mDL Implementation Guidelines.....	12
National mDL Deployment Landscape	13
Glossary of Key Terms	14
Related Toolkit Documents	14
Hardware & Software Requirements	16
Minimum Hardware Requirements	17
Software Requirements	17
Integration Architecture	18
CJIS Security Policy Requirements.....	19
Device Procurement Checklist	20
Related Toolkit Documents	20
Available Devices & Software	21
Smartphone Reader Applications.....	22
Purpose-Built & Ruggedized Hardware.....	23
Software, CAD/FBR & SDK Providers.....	24
Vendor Evaluation Framework	25
Related Toolkit Documents	25
Operational Workflows	26
Understanding the mDL Transaction.....	27
Traffic Stop: Step-by-Step Workflow	27
Downstream Report & Query Integration	28
Handling Common Failure Scenarios.....	29
Related Toolkit Documents	30
Procurement Considerations & Strategy	31
Procurement Planning Principles	32
Mandatory Requirements for Any Procurement.....	32
Suggested Contract Language.....	32
Adoption Pathway Options	33
Total Cost of Ownership	34
Related Toolkit Documents	34
Funding Strategies & Opportunities.....	36
Important Disclaimer.....	36
Overview and Funding Strategy	37
U.S. Department of Justice (DOJ) Grant Programs	38

U.S. Department of Homeland Security (DHS) / FEMA Grant Programs	42
U.S. Department of Transportation — FMCSA Grant Programs	43
U.S. Department of Transportation — NHTSA Highway Safety Grant Programs.....	43
State and Local Funding Sources	48
Congressional Appropriations Earmarks.....	49
Cooperative Purchasing Programs.....	50
Vendor Financing & OpEx Models	51
Grant Writing Tips for mDL Technology	52
Funding Program Quick Reference	53
Acronym Glossary	55
Related Toolkit Documents	57
Legal & Privacy Considerations.....	58
State Acceptance Law	58
Data Minimization and Selective Disclosure	60
Data Retention Policy	60
CJIS Security Policy	60
Fourth Amendment Considerations.....	61
Policy Development Checklist	61
Related Toolkit Documents	62
Training Plan Framework	63
Training Program Overview	64
Training Curriculum — Module Outlines	64
Delivery Format Recommendations	68
Competency Standards	69
Related Toolkit Documents	69
mDL Officer How-To Guide	71
Know Before You Go	72
How to Verify an mDL at a Traffic Stop	72
How to Use mDL Data in Your Reports.....	73
What to Do When Something Goes Wrong.....	74
What You Can and Cannot Do	74
Quick Reference — Traffic Stop at a Glance	75
Related Toolkit Documents	75
mDL FAQs for Law Enforcement	77
Introduction	78
Quick Reference	80
Related Toolkit Documents	80

About This Toolkit

The Law Enforcement mDL Technology Toolkit is a modular portfolio of standalone guidance documents designed to support law enforcement agencies at every stage of planning for and adopting ISO/IEC 18013-5 compliant Mobile Driver License (mDL) verification technology. Each document in the series stands alone and is designed for a specific audience — from frontline officers to procurement officers to legal counsel.

The toolkit was developed recognizing that different personnel within an agency need different information at different times. A training officer does not need the same level of technical detail as an IT director; a grant writer does not need the same operational guidance as a patrol sergeant. By structuring the toolkit as a series of modular documents, agencies can distribute exactly the right guidance to the right audience without requiring everyone to read a single large document.

Core Principle

It is not enough for an officer to simply read an mDL with a verifier device. The officer should be able to use a device to authenticate and read the mDL and then leverage that data to run additional queries and populate reports such as e-citations, crash reports, vehicle tow logs, and arrest reports. Every document in this series is written with that integrated workflow vision in mind.

How to Use This Toolkit

This Portfolio Overview document serves as the master index for the toolkit series. Use it to identify which documents are most relevant to your role or current planning phase. Each document is self-contained — you do not need to read other documents in the series to use any individual document, though cross-references are provided where relevant.

- Executives and command staff should begin with DOC-01 (Standards Overview) and DOC-07 (Legal & Privacy Considerations).
- Technology and IT officers should focus on DOC-02 (Hardware & Software Requirements) and DOC-03 (Available Devices & Software).
- Procurement and finance staff should review DOC-05 (Procurement) and DOC-06 (Funding).
- Training officers should use DOC-08 (Training Plan Framework) as the foundation for their agency's mDL training program.
- All patrol personnel and supervisors should receive DOC-04 (Operational Workflows) and DOC-09 (FAQ).

Document Series Index

Doc #	Title	Description	Primary Audience
-------	-------	-------------	------------------

DOC-01	Standards Overview	ISO/IEC 18013-5 & 18013-7, AAMVA guidelines, and the national mDL landscape	All Leaders & Technologists
DOC-02	Hardware & Software Requirements	Technical baseline specifications and integration architecture for compliant mDL verification	Technology Officers & IT Staff
DOC-03	Available Devices & Software	Market landscape of reader apps, ruggedized hardware, CAD/FBR providers, and SDKs	Procurement & Technology Officers
DOC-04	Operational Workflows	Step-by-step officer guidance for traffic stops, citations, arrests, and downstream data use	Officers, Supervisors & Training Staff
DOC-05	Procurement Considerations & Strategy	Solicitation requirements, contract language, adoption pathways, and total cost of ownership	Procurement Officers & Command Staff
DOC-06	Funding Strategies & Opportunities	DOJ (JAG/COPS/FEMA), USDOT/FMCSA (MCSAP, HP-ITD, HP-CMV, HP-ETS), NHTSA (Section 402, 405(c)), cooperative purchasing, and OpEx models	Grant Writers & Finance Staff
DOC-07	Legal & Privacy Considerations	State acceptance law, data minimization, CJIS compliance, and Fourth Amendment guidance	Legal Counsel & Command Staff
DOC-08	Training Plan Framework	Curriculum outline, delivery formats, and competency framework for agency-wide mDL training	Training Officers & Supervisors
DOC-09	mDL FAQ for Law Enforcement	Plain-language answers to the most common officer questions about mDL technology and procedures	All Law Enforcement Personnel

Planned Future Additions

The following resources are planned for inclusion in future versions of this toolkit:

- **DOC-10: Video Training Resource** — A short-form video demonstrating the mDL verification workflow for officer training
- **DOC-11: Agency Testimonials** — Case studies and first-person accounts from early-adopter law enforcement agencies
- **DOC-12: Vendor Comparison Matrix** — A side-by-side evaluation framework for comparing mDL reader solutions

Background: The mDL Landscape for Law Enforcement

Mobile Driver Licenses (mDLs) are digital representations of driver's license information stored securely on a holder's smartphone and presented via Bluetooth Low Energy (BLE), Near-Field Communication (NFC), or QR code. Unlike a photo of a physical license, a standards-compliant mDL is cryptographically signed by the issuing state DMV, making it substantially more resistant to fraud and counterfeiting than physical credentials.

As of April 2026, 21 U.S. states plus Puerto Rico have active mDL programs recognized by the Transportation Security Administration (TSA). An estimated 76% of Americans live in states that have adopted or are piloting mDL programs. Multiple identity credential service providers, as well as Apple Wallet, Samsung Wallet, and Google Wallet support mDLs in multiple states, dramatically accelerating the pace at which officers will encounter digital credentials during routine interactions.

Legislative Momentum

Georgia's HB 296 (2025) mandated that law enforcement officers accept mDLs during traffic stops when equipped with a reader, and required all Georgia law enforcement officers to receive mDL readers by July 1, 2027. Similar legislation is emerging in other states. Agencies that plan proactively will be better positioned than those that wait for a legislative mandate.

The Three-Party Model

Every mDL transaction involves three parties, and law enforcement officers fill the role of the Verifier (also called the Relying Party):

- **Holder:** The driver or pedestrian who possesses the mDL on their mobile device. The holder controls what data is shared and must actively consent to each transaction.
- **Issuing Authority:** The state DMV or equivalent agency that issued the credential and cryptographically signed it. The Issuing Authority's public keys, distributed through AAMVA's Digital Trust Service, allow any authorized reader to verify the credential's authenticity.
- **Verifier / Relying Party:** The law enforcement officer and their reader device. The verifier requests specific data elements, receives the holder's consent-gated response, and cryptographically validates the credential. The verifier never needs to handle the holder's device.

Key Standards Referenced in This Toolkit

Standard / Program	Relevance to Law Enforcement
ISO/IEC 18013-5:2021	Governs all in-person (proximity) mDL verification — the primary standard for traffic stops and field encounters. A revised edition (DIS) is in process.

ISO/IEC TS 18013-7:2025	Governs online/remote mDL verification. Relevant for future remote identification workflows and software systems with multi-year lifecycles.
AAMVA mDL Implementation Guidelines v1.6 (July 2026)	AAMVA's North America-specific guidance expanding on ISO/IEC 18013-5, defining data elements and privacy requirements for the U.S. and Canadian mDL ecosystem.
FBI CJIS Security Policy	Governs the handling of Criminal Justice Information by law enforcement systems — applies to any mDL reader or software that interfaces with NCIC/CIC queries or RMS data.
FMCSA MCSAP & High Priority Grant Programs	Federal Motor Carrier Safety Administration formula and competitive grants for CMV enforcement technology. Directly applicable to agencies with motor carrier inspection programs — mDL readers speed CDL verification and improve MCMIS inspection data quality.
NHTSA Section 402 & Section 405(c)	NHTSA highway safety formula grants administered through State Highway Safety Offices (SHSOs) and Traffic Records Coordinating Committees (TRCCs). Section 405(c) specifically funds crash data quality improvements — a direct fit for mDL-integrated crash reporting.
MMUCC — Model Minimum Uniform Crash Criteria (6th ed., 2025)	NHTSA's national standard for crash report data elements. mDL-sourced identity data in crash reports improves MMUCC compliance by eliminating manual transcription errors in critical fields.

Key Contacts & Resources

AAMVA Resources

- **AAMVA mDL Program Hub:** aamva.org/topics/mobile-driver-license
- **AAMVA mDL Implementation Guidelines v1.6:** aamva.org/getmedia/1bc1f2b3-bc7b-4e44-8112-127a4110ad94/mDLImplementationGuidelines-16.pdf
- **AAMVA mDL FAQ for Law Enforcement:** aamva.org/law-enforcement/mobile-driver-license-faq
- **AAMVA mDL Model Legislation:** aamva.org/policy/legislation/model-legislation
- **AAMVA Digital Trust Service:** aamva.org/topics/mobile-driver-license

Federal Resources

- **ISO/IEC 18013-5 Standard:** iso.org/standard/69084.html
- **FBI CJIS Security Policy:** le.fbi.gov/cjis-resources
- **DOJ Grants Program Plan:** justice.gov/dojgrantsprogramplan
- **BJA Funding Opportunities:** bjaojp.gov/funding/current
- **COPS Office Grants:** cops.usdoj.gov/grants

USDOT — FMCSA Resources

- **FMCSA Grant Programs Hub:** fmcsa.dot.gov/grants

- **MCSAP Formula Grant Program:** ai.fmcsa.dot.gov/Grants/MCSAP.aspx
- **HP-ITD Innovative Technology Deployment Grant:** ai.fmcsa.dot.gov/Grants/ITD.aspx
- **HP-CMV & HP-ETS High Priority Grants:** ai.fmcsa.dot.gov/Grants/HighPriority.aspx
- **FMCSA Grants Resource Center:** ai.fmcsa.dot.gov/Grants/ResourceCenter/Results

USDOT — NHTSA Resources

- **NHTSA Highway Safety Grants Program:** nhtsa.gov/highway-safety-grants-program
- **Section 405(c) Traffic Records Grant (via GHSA):** ghsa.org/resource-hub/section-405-national-priority-safety-program
- **Traffic Records Coordinating Committees (TRCCs):**
transportation.gov/government/traffic-records
- **MMUCC — Model Minimum Uniform Crash Criteria (6th ed.):**
crashstats.nhtsa.dot.gov (DOT HS 813 525a)
- **NHTSA Traffic Records Data Quality Management Guide:** crashstats.nhtsa.dot.gov (DOT HS 813 544)

Industry & Peer Organizations

- **IACP Policy Center:** theiacp.org/policycenter
- **Police Executive Research Forum (PERF):** policeforum.org
- **mDL Connection (Secure Technology Alliance):** mdlconnection.com

LAW ENFORCEMENT mDL TOOLKIT
DOC-01

Standards Overview

ISO/IEC 18013-5 & 18013-7, AAMVA Guidelines, and the National mDL
Landscape

Audience	Law Enforcement Leaders, Technology Officers, Command Staff
Purpose	Provides a plain-language explanation of the technical standards underlying mDL technology, their implications for law enforcement, and the current state of mDL deployment across the United States.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

What Is an mDL?

A Mobile Driver License (mDL) is a digital version of a state-issued driver's license or identification card that resides in a secure container on the holder's smartphone. Unlike a photo of a physical license or a simple barcode, a standards-compliant mDL is cryptographically signed by the issuing state DMV. This digital signature allows any authorized reader to verify — without contacting the DMV in real time — that the credential is authentic, has not been altered, and was issued by a trusted government authority.

An mDL is not a picture of a driver's license on a phone. It is an interactive credential that the holder actively presents, with data selectively shared only upon the holder's explicit consent. The holder's device must be unlocked and the holder must approve each transaction.

What mDL Is NOT

An mDL is not a screenshot, a PDF417 barcode scan, a photo, or a visual display of a license on a phone screen. Solutions requiring the holder to 'show' their screen carry significant fraud risk. This toolkit focuses exclusively on ISO/IEC 18013-5 compliant solutions that use cryptographic authentication.

ISO/IEC 18013-5: The In-Person mDL Standard

ISO/IEC 18013-5:2021 is the foundational international standard for mobile driver's licenses. It was published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It establishes the interface specifications for mDL presentation, authentication, and data exchange in proximity (in-person) scenarios — the primary use case for law enforcement.

A revised draft (ISO/IEC DIS 18013-5) is currently in the enquiry phase with ISO members and will replace the 2021 edition when finalized. Agencies should ensure procurement language requires compliance with the current version and includes provisions for updates.

Core Technical Components

Component	How It Works in Practice
Device Engagement	The mDL session is initiated when the officer's reader scans a QR code displayed on the holder's screen, or when the officer's reader device performs an NFC tap against the holder's phone. This establishes the encrypted communication channel.
BLE Data Transfer	After engagement, credential data is transferred over Bluetooth Low Energy (BLE). This is a short-range, encrypted wireless channel. The officer never needs to handle the holder's device.
Offline Operation	The entire transaction — engagement, transfer, and validation — can be completed with no internet connection. The credential data is stored on

	the holder's device and the reader validates it using pre-loaded public keys from AAMVA's Digital Trust Service.
Cryptographic Validation	The reader verifies the mDL's digital signature against the issuing state's public key. This confirms (a) the data was not altered since issuance, and (b) it was issued by a legitimate DMV.
Selective Disclosure	The officer's reader requests specific data elements (e.g., name, DOB, DL number). The holder's device presents only those fields. Address, vehicle restrictions, or other data not requested are not transmitted.
Holder Consent	The holder's device displays the data elements being requested and requires the holder to actively approve before any data is transmitted. The holder can deny the request.

Privacy Protections Built Into the Standard

ISO/IEC 18013-5 was explicitly designed with privacy as a core principle, not an afterthought. Key protections include:

- No centralized transaction logging — the standard does not include any mechanism for a central database of mDL verification events. Verification is peer-to-peer.
- No real-time DMV notification — when an officer reads an mDL, the issuing state's DMV is not notified. There is no "phone home" functionality in the standard itself.
- Selective disclosure — only the data elements requested and approved are transferred. The full credential is not exposed.
- Holder-controlled — the holder must actively unlock their device and approve every transaction.

Note on Privacy Risks

While the standard itself is privacy-protective, individual mDL wallet apps or reader software could be built with additional logging or data retention. Agencies should review vendor privacy policies and confirm that reader applications do not create surveillance capabilities beyond what is operationally necessary. See DOC-07 (Legal & Privacy Considerations) for detailed guidance.

ISO/IEC 18013-7: Online mDL Verification

ISO/IEC Technical Specification 18013-7:2025 extends the mDL framework to remote/internet-based verification scenarios. While the primary law enforcement use case remains proximity-based (in-person), Part 7 is relevant for agencies planning software systems with multi-year lifecycles.

AAMVA's mDL Implementation Guidelines v1.6 (July 2026) incorporated guidance for Part 7, including reference to the W3C Digital Credential (DC) API currently under development by the World Wide Web Consortium. Procurement language for any software expected to be in service beyond 2027 should reference both standards.

Feature	ISO/IEC 18013-5 (Part 5)	ISO/IEC 18013-7 (Part 7)
Scenario	In-person, proximity verification	Remote, internet-based verification
Primary LE Use Case	Traffic stop, arrest, field interview	Remote identity verification, online case management
Connectivity Required?	No — fully offline capable	Yes — internet connection required
Device Engagement	QR code or NFC tap	QR code / browser redirect / DC API
Data Transfer Protocol	Bluetooth Low Energy (BLE)	HTTPS / W3C DC API
LE Readiness	Deploy now — market solutions available	Emerging — include in long-term procurement planning

AAMVA mDL Implementation Guidelines

The American Association of Motor Vehicle Administrators (AAMVA) is the primary coordinating body for mDL programs across U.S. and Canadian jurisdictions. AAMVA's mDL Implementation Guidelines (current version: 1.6, July 2026) expand upon ISO/IEC 18013-5 to define the specific data elements, privacy requirements, and trust infrastructure applicable to the North American mDL ecosystem.

Compliance with AAMVA guidelines — not just ISO/IEC 18013-5 — is required for an mDL reader to be interoperable with the full range of U.S. and Canadian jurisdictions. Any reader that is only "ISO-compliant" without AAMVA DTS integration may fail to validate credentials from many states.

AAMVA Digital Trust Service (DTS)

AAMVA operates the Digital Trust Service — the infrastructure through which issuing authorities' public keys are distributed to verifiers. An mDL reader should receive mDL public keys from the DTS to cryptographically authenticate credentials from any state. Using public keys from the DTS, a reader can confirm whether an mDL was issued by a legitimate issuing authority, it was provisioned to the device being presented, and the data has not been tampered with or altered.

- All agencies procuring mDL reader solutions should confirm that the vendor is integrated with the AAMVA DTS.
- DTS integration should be verified during procurement, and vendors should provide documentation of current DTS integration status.

Key AAMVA Resources for Law Enforcement

- **mDL Implementation Guidelines v1.6 (July 2026):** aamva.org/topics/mobile-driver-license

- **mDL FAQ for Law Enforcement (January 2024):** aamva.org/law-enforcement/mobile-driver-license-faq
- **mDL Model Legislation:** aamva.org/policy/legislation/model-legislation
- **mDL Jurisdiction Map (live deployment tracking):** aamva.org/topics/mobile-driver-license

National mDL Deployment Landscape

As of April 2026, mDL adoption across the United States has reached a critical threshold. An estimated 76% of Americans live in states that have adopted or are piloting mDL programs.

States with Active TSA-Recognized mDL Programs (as of early 2026)

The following 21 states plus Puerto Rico have active mDL programs recognized by TSA for airport checkpoint use. Officers in these states have the highest immediate likelihood of encountering mDL holders:

State
Arizona
California
Colorado
Delaware
Georgia
Hawaii
Illinois
Iowa
Kentucky
Louisiana
Maryland
Montana
New Mexico
New York
North Dakota
Ohio
Puerto Rico
Utah
Virginia

West Virginia

Rapid Growth

The AAMVA mDL map is updated frequently as new jurisdictions complete deployment. Officers should expect to encounter mDLs from states other than their own — especially in jurisdictions near state borders or with high tourism and travel activity.

Glossary of Key Terms

Term	Definition
mDL	Mobile Driver License — a digital driver's license or state ID credential on a mobile device compliant with ISO/IEC 18013-5.
ISO/IEC 18013-5	The international standard governing in-person mDL presentation and verification. The primary standard for law enforcement mDL encounters.
ISO/IEC 18013-7	A technical specification extending 18013-5 for internet-based (online) mDL verification.
AAMVA	American Association of Motor Vehicle Administrators — coordinates mDL standards for North American jurisdictions.
DTS	AAMVA's Digital Trust Service — distributes Issuing Authority public keys to mDL verifiers.
BLE	Bluetooth Low Energy — the wireless protocol used for mDL data transfer between devices.
NFC	Near-Field Communication — short-range wireless technology used for mDL session initiation.
Selective Disclosure	The holder shares only the specific data elements requested — not the full credential.
Issuing Authority	The state DMV or equivalent agency that issues and digitally signs the mDL.
Relying Party / Verifier	The entity reading the mDL — in law enforcement contexts, the officer and their reader device.
PKI	Public Key Infrastructure — the cryptographic framework that enables mDL authentication.
mdoc	The ISO/IEC 18013-5 term for a signed digital document (mobile document) format used for mDLs and other credentials.

Related Toolkit Documents

- **DOC-02:** Hardware & Software Requirements — technical specifications for compliant readers
- **DOC-03:** Available Devices & Software — current market landscape
- **DOC-07:** Legal & Privacy Considerations — state law, data retention, CJIS, and Fourth Amendment
- **DOC-09:** mDL FAQ for Law Enforcement — plain-language answers to common officer questions

LAW ENFORCEMENT mDL TOOLKIT
DOC-02

Hardware & Software Requirements
Technical Baseline Specifications and Integration Architecture

Audience	Technology Officers, IT Staff, System Administrators
Purpose	Defines the minimum hardware and software requirements for ISO/IEC 18013-5 compliant mDL verification, describes integration architecture options, and outlines CJIS compliance obligations for law enforcement deployments.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

Minimum Hardware Requirements

Any device used to verify ISO/IEC 18013-5 compliant mDLs must support all three of the following communication technologies. These are non-negotiable technical minimums — a device lacking any one of them cannot establish a compliant mDL session.

Requirement	Technical Detail	Notes
Bluetooth Low Energy (BLE)	BLE 4.0 minimum; BLE 5.0 or higher recommended for range and stability. Required for the primary data transfer session.	Present on virtually all smartphones and tablets made after 2015
Near-Field Communication (NFC)	NFC ISO 14443 compliant. Used as one of two device engagement initiation methods. Range typically <4 cm.	Confirm NFC is enabled on device — some enterprise MDM profiles disable it
QR Code Reader (Camera)	Rear-facing camera with autofocus capable of scanning QR codes. Alternative to NFC for device engagement. Most modern smartphones qualify.	Some purpose-built scanners use integrated laser/imager instead of camera
Operating System	iOS 16.5 or later (iPhone 8 or later) for Apple devices; Android 8.0 or later for Android devices. Windows 10/11 for MCT-based solutions.	Confirm OS version requirements with specific reader app vendor
Cellular Connectivity (Conditional)	Not required for mDL verification itself, which operates offline. Required for CIC/NCIC queries and CAD/FBR data submission.	Vehicle-mounted hotspot can serve multiple officer devices

Verify NFC Separately From Hardware

A device may have NFC hardware but have it disabled by Mobile Device Management (MDM) policy or carrier settings. Before deploying reader apps, confirm NFC is enabled and accessible to third-party apps on every device in the fleet.

Software Requirements

Hardware alone is insufficient. The software stack running on the reader device must accomplish five distinct functions to provide a complete, operationally useful mDL verification capability:

Function	Description & Verification Question
mDL Session Management	Initiates the engagement (QR scan or NFC tap), negotiates the encrypted BLE session, requests specific data elements, receives the mDL response, and closes the session. ASK VENDOR: What

	engagement methods are supported? Is BLE session handling compliant with ISO/IEC 18013-5 Section 8?
Trust Chain Validation	Validates the mDL's digital signature against AAMVA's Digital Trust Service public keys. Without this, the software cannot confirm the credential is authentic. ASK VENDOR: Is the application using issuing authorities' public keys obtained from the AAMVA DTS?
Data Display & Photo Comparison	Presents parsed mDL data clearly to the officer, including the credential photo for identity comparison against the physical holder. ASK VENDOR: What data elements are displayed? Is the portrait/photo displayed? Are validity indicators shown?
Data Export / Integration	The most operationally critical capability: passing mDL data to CAD, FBR, RMS, and query systems. Without this, officers must re-enter data manually. ASK VENDOR: What API, SDK, or integration mechanism is available? Which CAD/FBR systems are already integrated?
CJIS Compliance	Any software interfacing with Criminal Justice Information must comply with the FBI CJIS Security Policy. ASK VENDOR: Provide your CJIS Security Policy compliance documentation and your current CJIS Information Security Agreement (ISA).

Integration Architecture

The decision of how to deploy mDL readers within your existing technology stack is the single most important infrastructure planning decision. Two primary architectures exist:

Architecture A: Unified Device (Long-Term Integration)

A single ruggedized device — such as a 2-in-1 tablet, purpose-built handheld, or future-generation MCT — serves as both the mDL reader and the officer's primary computing terminal. The CAD/FBR/RMS software and the mDL reader application either run natively together or communicate directly on the same device OS.

Advantages	Considerations
Single device to manage, provision, and support	Requires CAD/FBR/RMS vendor to support mDL integration natively or via SDK
No data hand-off between devices — reduced failure points	May require a new or upgraded MCT device if existing hardware lacks BLE/NFC
Streamlined officer workflow — one screen, one tool	Procurement and deployment timeline tied to CAD/FBR vendor integration roadmap
Lowest total cost of ownership at scale	Transition planning needed if replacing existing MCT fleet

Architecture B: Two-Device Workflow (Available Now)

A smartphone or standalone mDL reader device reads the mDL, then transfers data to the in-vehicle MCT or laptop via Bluetooth pairing, local Wi-Fi, or a vendor-provided data sharing mechanism. The officer runs queries and populates reports on the MCT using the transferred data.

Advantages	Considerations
Deployable immediately without modifying MCT/CAD software	Data hand-off reliability between devices must be confirmed in testing
Preserves existing MCT investment	Some manual re-entry may still be required for non-integrated fields
Lower initial procurement cost	Two devices per officer to manage, charge, and support
Allows agencies to begin mDL acceptance while long-term integration is planned	Higher total cost of ownership over time vs. unified device

CJIS Security Policy Requirements

The FBI Criminal Justice Information Services (CJIS) Security Policy governs the handling, storage, and transmission of Criminal Justice Information (CJI). Any mDL reader software that connects to, transmits data to, or receives data from CJIS systems — including CAD, RMS, NCIC, and state criminal history databases — must comply.

Key CJIS requirements relevant to mDL deployments include:

- **Encryption:** All CJI data in transit must be encrypted. Confirm the reader app – if directly integrated with CJIS-connected software or hardware - and any integration middleware use FIPS 140-2 compliant encryption.
- **Multi-Factor Authentication:** Access to systems containing CJI requires advanced authentication. Confirm MFA is implemented for officer login to integrated systems.
- **Audit Logging:** All access to CJI must be logged with user ID, timestamp, and action. Confirm the system maintains audit logs meeting CJIS requirements.
- **Personnel Security:** Personnel with unescorted access to CJI must have appropriate background checks. This includes vendor employees with system access.
- **Information Security Agreement:** All vendors accessing or processing CJI must execute a CJIS Information Security Agreement (ISA). Require this from all mDL reader software vendors before contract execution.

CJIS Compliance Is Non-Negotiable

An mDL reader that connects mDL data directly to NCIC/CIC queries or populates fields directly into an RMS must comply with CJIS Security Policy. Failure to enforce this requirement exposes the agency to potential loss of CJIS access. All vendor contracts should include CJIS ISA requirements, and compliance should be verified before deployment.

Device Procurement Checklist

Use this checklist when evaluating any hardware device for mDL reader deployment:

- ☐ Bluetooth Low Energy 4.0 or higher confirmed and enabled
- ☐ NFC capability confirmed and enabled (not disabled by MDM or carrier)
- ☐ Rear-facing camera with QR code scanning capability confirmed
- ☐ Operating system meets reader app vendor's minimum version requirement
- ☐ Device form factor appropriate for law enforcement field use (drop resistance, weather resistance, screen readability in sunlight)
- ☐ Battery life adequate for a full shift without recharging
- ☐ MDM/EMM compatibility confirmed for agency device management platform
- ☐ Integration path to CAD/FBR/MCT confirmed with software vendor

Related Toolkit Documents

- **DOC-01:** Standards Overview — detailed explanation of ISO/IEC 18013-5 technical components
- **DOC-03:** Available Devices & Software — current vendor market landscape
- **DOC-05:** Procurement Considerations & Strategy — solicitation language and contract requirements

LAW ENFORCEMENT mDL TOOLKIT

DOC-03

Available Devices & Software

Market Landscape of mDL Reader Apps, Hardware, and CAD/FBR Providers

Audience	Procurement Officers, Technology Officers, Command Staff
Purpose	A current, non-exhaustive survey of commercially available hardware devices, smartphone applications, software platforms, and SDKs capable of reading and leveraging ISO/IEC 18013-5 compliant mDL data. Includes due diligence questions for each vendor category.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

This document reflects the market as of April 2026. The mDL reader market is evolving rapidly. Agencies should conduct their own market research and directly confirm product capabilities, AAMVA DTS integration status, and CJIS compliance before procurement.

Disclaimer

Inclusion of a vendor in this document does not constitute an endorsement by AAMVA or any law enforcement agency. Agencies should conduct independent evaluation and due diligence before purchasing any product. All vendor capabilities should be confirmed directly with the vendor.

Smartphone Reader Applications

These applications run on commercially available iOS or Android smartphones and provide ISO/IEC 18013-5 compliant mDL reading capability. They represent the fastest path to initial deployment for agencies without existing mDL hardware infrastructure.

Developer	Application Name	Platform	LE Integration	Website
Credence ID	Tap2iD	iOS / Android	SDK available for LE integration	credenceid.com
GET Group	GET Mobile Verify	iOS / Android	LE-focused solution	mobiledl.us
Scytales	ISO Mobile Verifier	iOS / Android	Confirm with vendor	scytales.com
Idemia	Mobile ID Verify	iOS / Android	LE-focused solution	idemia-mobile-id.com
AZ DOT	Smart ID Verifier	iOS / Android	State-issued app	azdot.gov
Maryland MDOT	Mobile ID Check by MD	iOS / Android	State-issued app	mva.maryland.gov
CA DMV (SpruceID)	mDL Reader — CA DMV Wallet	iOS / Android	State-issued app	dmv.ca.gov
IDScan.net	VeriScan (mDL-capable)	iOS / Android / Windows	Enterprise integration available	idscan.net
OneProof	ONEPROOF MOBILE SDK	iOS/Android/Linux/Windows	LE-Focused Solution.	OneProof

Due Diligence Questions — Reader Apps

- Is the application compliant with ISO/IEC 18013-5 and AAMVA mDL Implementation Guidelines (current version)?
- Is the application integrated with AAMVA's Digital Trust Service?
- What data elements are requested and displayed? Can requested elements be configured per agency?
- Does the application log transactions locally on the device? If so, how long, and how is data purged?
- What CAD/FBR/RMS systems is the app currently integrated with? What is the integration mechanism (API, SDK, export)?
- Is a CJIS Information Security Agreement available for execution?

Purpose-Built & Ruggedized Hardware

The following manufacturers produce hardware devices with BLE, NFC, and camera capabilities suitable for law enforcement field deployment. Ruggedized form factors are strongly recommended for patrol use.

Manufacturer	Description	Website
Credence ID	Tap2ID Verifier — purpose-built handheld mDL reader with integrated NFC, BLE, and camera designed for identity verification workflows	credenceid.com
Panasonic (Public Safety)	TOUGHBOOK series — MIL-SPEC ruggedized Windows laptops, 2-in-1 devices, tablets, and smartphones purpose-built for public safety; NFC and BLE capable	connect.na.panasonic.com
Getac	MIL-SPEC ruggedized laptops, tablets, and handheld devices with NFC and BLE capabilities for demanding field environments	getac.com
Dell Latitude Rugged	Windows ruggedized PCs, 2-in-1 convertibles, and tablets suitable for vehicle-mounted and handheld LE deployment	dell.com
Zebra Technologies	Ruggedized mobile computers, handheld scanners, and tablets for public safety; strong MDM/EMM ecosystem	zebra.com
L-Tron	In-car and on-person DL/mDL reader devices — PDF417 barcode scanners with ISO mDL reader capability designed for integration with in-vehicle MCT/CAD systems	l-tron.com
Apple iPhone / iPad	iOS devices (iPhone 8 or later with iOS 16.5+) serve as reader platforms when running compliant reader apps; NFC and BLE capable	apple.com
Android Smartphones / Tablets	Android devices (8.0 or later) with NFC and BLE serve as reader platforms when running compliant	Various manufacturers

	reader apps; wide range of ruggedized Android options available from multiple manufacturers	
OneProof	Devices for In-Car, Handheld Android Devices custom build for Law Enforcement for both In-Person and DL/MDL reader with PDF417 + mDL + ePassport with specific design to integrate with Vehicle and Law enforcement Solutions.	OneProof

Software, CAD/FBR & SDK Providers

The following software platforms are known to AAMVA to currently offer either CAD/FBR environments with mDL data ingestion, developer SDKs enabling mDL integration into existing systems, or both. This is the most critical vendor category for agencies seeking full workflow integration.

Vendor	Description	Website
SmartCop	SmartMobile, SmartMCT, and Mobile Forms platforms — actively supports mDL data ingestion for auto-populating e-citations, crash reports, arrest reports, and other LE forms. One of the most mature LE mDL integrations available.	smartcop.com
Credence ID	Tap2iD SDK — developer toolkit enabling third-party LE software vendors to build ISO/IEC 18013-5 compliant mDL reading directly into existing applications without building the reader stack from scratch.	credenceid.com
Munio	Munio provides law enforcement agencies with a secure, ISO-compliant solution for verifying digital driver's licenses (mDLs) in the field.	munio.co/law-enforcement
OneProof	ONEPROOF SDK or Custom SDK designed to integrate with existing solutions to provide ability to accept mDL's.	OneProof
Signal 8 Systems	Smart Squad Mobile Application for Digital Driver's License	Smart Squad App

Active Development — Vendor Categories to Monitor

The following vendor categories should be monitored and queried for current status during any procurement process:

- Major CAD/RMS/FBR providers (Mark43, CentralSquare, Motorola PremierOne, etc.) — all large LE software vendors should be asked about mDL integration roadmaps

- Body camera / evidence management platform vendors — integration of mDL data with body camera footage metadata is an emerging capability
- e-Citation platform vendors — direct mDL data ingestion into citation forms is a natural integration point
- State-issued reader apps — many state DMVs are publishing or have published their own reader apps specifically for LE use within their jurisdiction

Vendor Evaluation Framework

When evaluating any mDL reader vendor, agencies should request documented answers to the following questions before procurement:

Compliance & Standards	Integration & Operations
• ISO/IEC 18013-5 compliance documentation • AAMVA mDL Implementation Guidelines compliance • AAMVA DTS enrollment and sync status • CJIS Information Security Agreement availability • FedRAMP or StateRAMP authorization (if cloud-hosted)	• Current CAD/FBR/RMS integration partnerships • API/SDK availability and documentation • Data ownership provisions • Multi-jurisdiction credential support scope • ISO/IEC 18013-7 roadmap for online verification

Related Toolkit Documents

- **DOC-02:** Hardware & Software Requirements — technical specifications to verify against vendor claims
- **DOC-05:** Procurement Considerations & Strategy — solicitation language and evaluation criteria

LAW ENFORCEMENT mDL TOOLKIT

DOC-04

Operational Workflows

Step-by-Step Officer Guidance for mDL Verification

Audience	Patrol Officers, Supervisors, Field Training Officers
Purpose	Provides practical, scenario-based guidance for law enforcement officers on how to verify ISO/IEC 18013-5 compliant mDLs during traffic stops and other field encounters, and how mDL data integrates into downstream reporting workflows.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

Read Before Deploying

Officers should not use this guidance until their agency has formally deployed a compliant mDL reader application and provided training on its specific use. This document describes general workflow principles applicable to ISO/IEC 18013-5 compliant solutions. Specific steps may vary based on the reader application and CAD/FBR system your agency uses.

Understanding the mDL Transaction

Before walking through specific scenarios, officers should understand three fundamental principles that govern every mDL interaction:

- **You will never need to handle the holder's phone.** All data transfer occurs wirelessly. The holder keeps their device. This is both an officer safety advantage and a privacy protection.
- **The holder must actively consent.** The holder's device will display what data you are requesting and require them to approve it before anything is transmitted. If they decline, the transaction ends.
- **The credential is cryptographically validated, not just displayed.** Your reader verifies the digital signature from the issuing DMV. A valid result means the data is authentic — not just visually convincing.

Traffic Stop: Step-by-Step Workflow

Phase 1: Pre-Approach

1. Complete standard pre-stop procedures (radio, CAD entry, etc.) per agency policy.
2. Activate your mDL reader application on your reader device before or during your approach to the vehicle. Having the app ready reduces dwell time at the vehicle window.
3. If using a two-device workflow (smartphone reader + MCT), confirm the reader device is paired and ready to transfer data to your MCT.

Phase 2: Initial Contact

4. Make initial contact with the driver using standard protocol.
5. Request identification. If the driver states they have an mDL: inform them you will read it wirelessly and they should open their mDL wallet app (Apple Wallet, Google Wallet, or their state's app). The driver does not need to hand you their device.
6. If the driver offers a physical credential, accept it and process normally — do not require them to produce an mDL instead.

Phase 3: mDL Verification

7. Ask the driver to display the QR code in their mDL app, or hold their device near your reader for NFC (depending on the method your reader app uses).

8. Scan the QR code or complete the NFC tap. Your reader app will establish an encrypted Bluetooth connection with the driver's device.
9. Your reader app will display a consent screen on the driver's device showing what data you are requesting. The driver must approve. If they decline, you cannot proceed with mDL verification — fall back to physical credential if available.
10. Once the driver approves, your reader app will display the verified credential data, including the driver's photo. Compare the photo to the person in front of you.
11. Check the validity indicators displayed by your reader app — license status (valid, suspended, revoked, expired), expiration date, and any displayed restrictions or endorsements.

Phase 4: Data Integration & Downstream Actions

12. If your reader app is integrated with your CAD/FBR system, mDL data should auto-populate the active incident, query fields, and any open report forms. Confirm the data populated correctly.
13. If using a two-device workflow, transfer or export the mDL data to your MCT per your agency's procedure.
14. Submit CIC/NCIC queries using the DL number captured from the mDL — this eliminates transcription errors that can cause missed hits.
15. Complete the stop using standard procedures. Issue citation, warning, or take other appropriate action. mDL data should auto-populate the citation form if your reader is integrated.

Officer Safety Advantage

An officer can verify an mDL from outside the vehicle window using QR scan from a safe distance. Some reader deployments support BLE engagement that can initiate from several feet away. Agencies should explore long-range engagement options to keep officers out of the window line as long as possible, while ensuring they are interacting with the correct mDL (i.e. differentiating between the driver's mDL vs. a vehicle passenger).

Downstream Report & Query Integration

The full value of mDL technology is realized when credential data flows automatically to downstream systems. The following table describes how mDL data supports specific officer actions:

Action	mDL Data Benefit	Without Integration
e-Citation	Name, address, DOB, DL number, and license class auto-populate citation fields	Officer manually reads and types all fields — error-prone and time-consuming

Crash/Accident Report	All involved party identity fields auto-populated; DL status confirmed at time of crash	Manual transcription from physical credential under stress conditions
CIC/NCIC Query	DL number auto-submitted — eliminates transcription errors that cause missed hits on wanted persons	Officer manually reads DL number aloud or types — common source of errors
Arrest Report	Booking identity data sourced from cryptographically verified credential — reduces identity fraud at intake	Risk of incorrect identity data entering booking records
Vehicle Tow Log	Driver identity captured at time of tow for accurate record and notification	Manual data entry, often completed after the fact from memory or notes
Field Interview / Contact	Person contact accurately captured and linked to RMS master name index	Manual entry; subject may provide false information that goes unchallenged
DUI/DWI Investigation	Accurate subject identity and license status captured at initial contact; linked through investigation	Additional steps required to confirm identity and license status under time pressure

Handling Common Failure Scenarios

Officers will regularly encounter situations where standard mDL verification cannot be completed. The following guidance covers the most common scenarios:

Holder's Device Has No Battery / Is Damaged

Treat the same as a driver without a physical credential. If the driver has a physical credential, process normally. State law in most jurisdictions still requires drivers to carry a physical credential; verify your jurisdiction's current legal requirement.

Reader Cannot Establish Session (Technical Failure)

Fall back to physical credential verification or standard identification procedures. Document the reader failure and report it to your technology contact for troubleshooting.

Out-of-State or International mDL

Any ISO/IEC 18103-5 compliant reader should be able to validate mDLs from all 21+ participating U.S. jurisdictions so long as it has the jurisdictions' public keys. Your reader app should display the issuing state clearly. For international mDLs, check whether your reader app has international trust chain support — coverage varies by vendor.

Driver Declines to Share mDL Data

The holder has the right to decline the consent prompt on their device. If the driver declines: request their physical credential. If they have no physical credential, follow your agency's standard protocol for a driver without identification.

Reader Displays an Authentication Warning or Failure

If your reader app displays a warning that the credential cannot be authenticated (invalid signature, expired trust chain, etc.), do not treat the credential as valid. Document the failure. Treat the situation as if no valid credential was presented and follow agency policy. Do not attempt to manually verify a credential that your reader has flagged as potentially invalid.

Related Toolkit Documents

- **DOC-01:** Standards Overview — how the technology works
- **DOC-08:** Training Plan Framework — officer training curriculum
- **DOC-09:** mDL FAQ for Law Enforcement — quick answers to common questions

LAW ENFORCEMENT mDL TOOLKIT

DOC-05

Procurement Considerations & Strategy

Solicitation Requirements, Contract Language, and Adoption Pathways

Audience	Procurement Officers, Technology Officers, Command Staff, Contract Administrators
Purpose	Provides a framework for law enforcement agencies to plan and execute the procurement of ISO/IEC 18013-5 compliant mDL reader hardware and software, including mandatory requirements, suggested contract language, adoption pathway options, and total cost of ownership guidance.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

Procurement Planning Principles

Procuring mDL verification technology requires balancing the urgency of immediate deployment (officers are already encountering mDL holders) with the strategic goal of full integration into existing CAD/FBR/RMS environments. Agencies that rush to deploy standalone readers without planning for integration may find themselves investing twice — once for the initial tool, and again for future integrations that can be contemplated and planned for now.

The guiding principle for all mDL procurement should be: acquire the capability that meets today's operational need while explicitly building the integration path into the contract.

Mandatory Requirements for Any Procurement

These requirements should appear as mandatory (pass/fail) criteria in all solicitations for mDL reader hardware or software. Proposals that do not meet all mandatory requirements should not advance to evaluation.

Requirement	Verification Method
ISO/IEC 18013-5 compliance (current version)	Vendor must provide compliance documentation or third-party certification. Specify requirement for update to future versions.
AAMVA mDL Implementation Guidelines compliance (current version)	Vendor must confirm and document compliance with current AAMVA guidelines, including data element handling and DTS integration.
AAMVA Digital Trust Service integration	Vendor must demonstrate active DTS use and confirm trust material is kept current. Test with credentials from at least three different states.
CJIS Security Policy compliance (for any system touching CJI)	Vendors proposing solutions that directly connect to CJIS systems and data must provide executed CJIS ISA or confirm willingness to execute before contract award. Review compliance documentation.
BLE, NFC, and QR engagement all supported	Demonstrate all three engagement methods in a technical demonstration. Test in the actual deployment environment (vehicle, outdoor conditions).
Data ownership — agency retains all transaction data	Include explicit data ownership language in contract. Vendor must deliver all agency data upon contract completion or termination.

Suggested Contract Language

Solicitation Standards Reference Language

"The offered solution shall be compliant with ISO/IEC 18013-5 (current version) and AAMVA's mDL Implementation Guidelines (current version) for in-person (proximity) mDL

verification, and shall support all device engagement methods specified therein (NFC, QR Code, and Bluetooth Low Energy). For software systems with a projected deployment lifecycle extending beyond 2027, the solution shall additionally comply with or provide a documented roadmap for compliance with ISO/IEC 18013-7 (online mDL verification). The vendor shall maintain synchronization with AAMVA's Digital Trust Service throughout the contract term. Any software component that stores, transmits, or interfaces with Criminal Justice Information shall comply with the FBI CJIS Security Policy, and the vendor shall execute a CJIS Information Security Agreement prior to contract execution. All data elements captured, stored, or transmitted through the offered solution shall be the property of [Agency Name], and the vendor shall deliver a complete export of all agency data upon contract completion, modification, or termination."

Adoption Pathway Options

Option A: Immediate Deployment — Smartphone Reader App

Deploy a compliant mDL reader application on agency-issued smartphones. This is the fastest path to mDL verification capability.

Benefits	Limitations
Can deploy in weeks, not months	Requires manual data re-entry into CAD/FBR without integration
Leverages existing device fleet (if smartphones issued)	Does not solve the core integration need long-term
OpEx model available — monthly per-device pricing	May create two-device workflow if smartphones are separate from MCT
Demonstrates capability to leadership while full integration is planned	Training must address both the reader app AND the manual data transfer workflow

Option B: Purpose-Built Portable Reader + MCT Integration

Deploy a dedicated portable mDL reader that can be worn or carried by an officer and that interfaces with the existing in-vehicle MCT. The reader captures the mDL and passes data to the MCT via the reader's integration interface.

- **Best for:** Agencies with a stable MCT/CAD environment where the MCT vendor does not yet offer native mDL integration but is capable of accepting data from a peripheral reader device.
- **Procurement note:** Require the handheld reader vendor and MCT/CAD vendor to both certify the integration in writing before award. Do not accept a statement that integration is 'possible' — require a demonstrated, tested integration.

Option C: Integrated CAD/FBR/MCT with Native mDL Support (Long-Term)

Incorporate mDL verification capability into the next planned hardware and software refresh cycle. Require any new CAD/FBR/RMS contract to include mDL integration as a mandatory deliverable.

- **Best for:** Agencies within 12-24 months of a CAD/FBR or MCT hardware refresh. Plan the mDL requirement now to ensure it is included in the next RFP.
- **Key action:** Contact your current CAD/FBR/RMS vendor now and ask about their mDL integration roadmap. Include mDL capability as a rated criterion in your next contract renewal or re-procurement.

Total Cost of Ownership

Agencies should evaluate mDL reader solutions on total cost of ownership over a 3-5 year lifecycle, not just initial acquisition cost. The following table identifies the full cost components to include in any cost analysis:

Cost Component	CapEx Model	OpEx / DaaS Model
Hardware Acquisition	One-time upfront purchase; agency owns devices	Monthly per-device fee; vendor owns devices
Software Licensing	Annual maintenance/license fees after initial purchase	Included in monthly subscription (confirm scope)
Cellular Data Plan	Monthly data plan per device	Often bundled — confirm data caps
Integration Development	One-time (or per-version) development cost to connect reader to CAD/FBR	May or may not be included — clarify upfront
Training (Initial + Ongoing)	Include in contract as a deliverable	Include in contract as a deliverable
Hardware Refresh / Replacement	Budget for ~30% annual replacement (loss, damage, failure)	Typically included in DaaS — confirm refresh cycle
AAMVA DTS Access	Confirm whether included in vendor pricing or separately billed	Confirm whether included in vendor pricing or separately billed

Related Toolkit Documents

- **DOC-03:** Available Devices & Software — current vendor landscape for market analysis
- **DOC-06:** Funding Strategies — grant programs and alternative funding for procurement
- **DOC-07:** Legal & Privacy Considerations — contract and legal requirements to include in solicitations

LAW ENFORCEMENT mDL TOOLKIT

DOC-06

Funding Strategies & Opportunities

DOJ, USDOT/FMCSA, NHTSA, State Programs, Cooperative Purchasing, and OpEx Models

Audience	Grant Writers, Finance Officers, Command Staff
Purpose	Identifies and describes the full range of funding mechanisms available to law enforcement agencies for acquiring mDL reader hardware, software, integration services, and training — including DOJ criminal justice grants, USDOT/FMCSA commercial vehicle safety grants, NHTSA highway safety and traffic records grants administered through state highway safety offices, cooperative purchasing vehicles, and alternative financing models.
Published	MM/YYYY American Association of Motor Vehicle Administrators (AAMVA)

Important Disclaimer

This document is intended to serve as general guidance to assist law enforcement agencies in identifying potential funding opportunities for mDL reader technology. It is not an authoritative legal or financial resource and should not be relied upon as such.

Grant program availability, eligibility requirements, funding levels, application deadlines, and allowable uses are subject to change with each fiscal year and are determined by Congressional appropriations, agency rulemaking, and individual Notice of Funding Opportunity (NOFO) documents. Information in this document may not reflect the most current program requirements.

Before initiating any grant application, agencies are strongly advised to: (1) consult the official NOFO published on Grants.gov or the administering agency's website for the current fiscal year; (2) contact the administering agency's grants management office directly to confirm eligibility and allowable uses; (3) engage your state's designated pass-through agency for formula programs; and (4) consult qualified legal and financial counsel as appropriate.

AAMVA makes no representations or warranties regarding the accuracy, completeness, or currency of the funding information contained in this document. References to specific programs, funding amounts, deadlines, or agency contacts are provided for informational purposes only.

Overview and Funding Strategy

mDL reader technology sits at the intersection of criminal justice, commercial vehicle safety, highway safety, and transportation technology — a rare characteristic that opens funding eligibility across multiple federal agencies simultaneously. Agencies are encouraged to pursue a blended strategy, matching each cost component (hardware, software, integration, training) to the most appropriate funding source.

Core Funding Strategy Principle

Because mDL readers serve multiple missions — general law enforcement, motor carrier enforcement, and traffic crash data quality — the same deployment may be justifiable under DOJ, FMCSA, and NHTSA grant programs. Agencies with motor carrier inspection units should explore FMCSA channels in parallel with DOJ channels, and coordinate with their state highway safety office on crash data quality angles. A blended multi-source strategy both increases total available funding and reduces dependency on any single grant program.

Understanding Grant Types: Formula, Competitive, and Invitational

Before pursuing any grant program, agency staff must understand the fundamental differences in how each type of funding is accessed. Misunderstanding this structure is the single most common cause of wasted grant writing effort.

Grant Type	How Agencies Access It	Examples in This Document
Formula (Non-Competitive)	Allocated to states by statutory formula (population, road miles, etc.). States sub-award to eligible local agencies through annual solicitation processes. No	JAG (formula portion), NHTSA Sec. 402, NHTSA Sec. 405(c), MCSAP, HSGP/SHSP, SLCGP

	competition with other agencies nationally.	
Competitive (Discretionary)	Agencies apply directly and compete nationally or regionally. Awards are based on merit, project design, and alignment with program priorities.	HP-CMV, HP-ITD, BWC Policy & Implementation Program, NIJ Demonstration
Invitational (Earmark)	Agency MUST be specifically named in a Congressional appropriations document (the Joint Explanatory Statement). No open competition. Requires proactive Congressional engagement.	COPS TEP — see note in that section

Note on Funding Availability

Funding levels, deadlines, and program details vary from fiscal year to fiscal year based on Congressional appropriations. Always consult the current Notice of Funding Opportunity (NOFO) on Grants.gov or the administering agency's website for current figures before preparing an application.

U.S. Department of Justice (DOJ) Grant Programs

Edward Byrne Memorial Justice Assistance Grant (JAG) Program

The JAG program is the broadest and most accessible federal funding source for state and local law enforcement technology. Administered by the Bureau of Justice Assistance (BJA), JAG funds can cover mDL reader hardware, software licenses, CAD/FBR integration development, and officer training. With no matching funds requirement for formula awards and broad eligible use categories, JAG is typically the first funding source agencies should pursue.

Detail	Information
Administering Agency	Bureau of Justice Assistance (BJA), U.S. Department of Justice
Grant Type	Formula (non-competitive, state/local allocation) and Discretionary (competitive). Most agencies access formula funds through their State Administering Agency (SAA).
Eligible Uses for mDL	Law enforcement equipment and technology; criminal justice information sharing systems; officer training; planning, evaluation, and technology improvement programs
Match Requirement	None for formula JAG. Verify for any discretionary solicitation.
Application Path	Formula: through your State Administering Agency (SAA) — contact your state's SAA to identify current solicitation cycles and deadlines. Discretionary: justgrants.usdoj.gov

JAG Purpose Areas	For mDL projects, cite: 'Law Enforcement Programs' and 'Planning, Evaluation, and Technology Improvement Programs.' For CMV-focused mDL readers, also cite 'Law Enforcement Equipment.'
Website	bia.ojp.gov

✓ Grant Writing Tip — JAG

Clearly articulate the operational problem: officers encountering mDLs without tools to read them; manual data entry errors causing missed criminal hits during NCIC queries; re-entry time that reduces patrol capacity. Quantify where possible: number of officers receiving readers, estimated time savings per stop, projected reduction in data entry errors. Reference AAMVA data on state mDL adoption rates to show the problem is growing — officers will encounter mDLs whether the agency is ready or not.

COPS Office Technology Programs

The Office of Community Oriented Policing Services (COPS) has invested over \$20 billion in policing since 1994. Two COPS programs are relevant to mDL technology, with very different eligibility structures.

Technology and Equipment Program (TEP) — Invitational/Earmark

⚠ Important — COPS TEP Is Not an Open Competition

COPS TEP is a noncompetitive, invitational program. To be eligible, your agency must be specifically named in the Congressional Joint Explanatory Statement (JES) accompanying the annual Commerce, Justice, Science, and Related Agencies Appropriations Act. Agencies not in the JES cannot apply regardless of project merit. Agencies seeking future inclusion should engage their congressional delegation proactively — see the Strategy for Unlisted Agencies row in the table below.

Detail	Information
Administering Agency	COPS Office, U.S. Department of Justice
Grant Type	Noncompetitive, Invitational (earmark). Named agencies only. No local match requirement.
Eligible Applicants	ONLY agencies named in the current fiscal year's Congressional Joint Explanatory Statement (JES) under 'COPS Technology and Equipment Community Projects / COPS Law Enforcement Technology and Equipment.'
Strategy for Unlisted Agencies	Contact your U.S. House and Senate offices. Congressional staff handle appropriations requests; submit a concise project

	description and cost estimate. Requests for the following fiscal year are typically due to congressional offices in January–February. Engage your state's law enforcement association to support multi-agency requests.
Website	cops.usdoj.gov/tep

Community Policing Development (CPD) Microgrants

Detail	Information
Administering Agency	COPS Office, U.S. Department of Justice
Grant Type	Competitive
Eligible Uses for mDL	Innovative community policing strategies. mDL readers that reduce friction in officer-community interactions (faster, less intrusive verification) may qualify under the technology innovation category.
Match Requirement	Verify in current NOFO
Availability Note	This program's availability varies by fiscal year; it has been zeroed out in some years. Confirm current status on the COPS website before investing application effort.
Website	cops.usdoj.gov/grants

BJA Body-Worn Camera Policy and Implementation Program (BWCIIP)

The BWCIIP is included as a creative but legitimate nexus for agencies that already operate or plan to launch body-worn camera programs.

The BJA BWCIIP is a competitive grant program that funds law enforcement and correctional agencies in piloting, establishing, or expanding body-worn camera programs. For agencies with active BWC deployments, mDL reader technology has a genuine evidence management nexus: mDL data captured during a stop becomes part of the digital evidence record associated with BWC footage, improving chain-of-custody documentation and data integrity.

Detail	Information
Administering Agency	Bureau of Justice Assistance (BJA), U.S. Department of Justice
Grant Type	Competitive

Eligible Uses for mDL	Digital evidence management integration; streamlining transfer of digital evidence from law enforcement to prosecutors; cross-agency evidence sharing and data integration
mDL Nexus	mDL data captured at point of contact (cryptographic identity, license status, photo) is timestamped digital evidence linked to the BWC footage of the same encounter. mDL-BWC integration strengthens evidentiary foundation and chain-of-custody documentation. Frame as 'digital evidence management and integration.'
Match Requirement	None for most categories — verify in current NOFO
Website	bja.ojp.gov — search Body-Worn Camera Partnership Program

✓ Grant Writing Tip — BWCIIP

Frame mDL reader procurement as a 'digital evidence capture and management' investment, not merely an identity verification tool. The key narrative: when an officer reads an mDL, the cryptographically authenticated identity data and license status is timestamped and linked to the concurrent BWC footage — creating a more complete, more defensible evidentiary record than manual notation. Cite BWCIIP program objectives around improving the evidentiary value of BWC footage and streamlining evidence transfer to prosecutors.

NIJ Technology Demonstration Grants

NIJ demonstration grants are a pilot-site pathway especially valuable for agencies willing to generate performance data for the broader law enforcement community.

The National Institute of Justice (NIJ), the research, development, and evaluation arm of the DOJ, funds technology demonstration and evaluation projects. For agencies willing to serve as a structured pilot site for mDL acceptance technology, NIJ grants provide both funding and a national platform for disseminating results.

Detail	Information
Administering Agency	National Institute of Justice (NIJ), U.S. Department of Justice
Grant Type	Competitive
Relevant Programs	Law Enforcement Technology (LET) research and evaluation grants; Science and Technology funding opportunities. Monitor nij.ojp.gov/funding/current for open solicitations.

Eligible Uses for mDL	Pilot-site implementation and structured evaluation of mDL verification technology; development of performance metrics and best practices; officer workflow and safety impact studies
Strategic Value	NIJ-funded demonstration projects generate published performance data that strengthens future JAG, NHTSA, and FMCSA grant applications. Serving as an NIJ pilot site also generates national visibility and establishes the agency as a technology leader.
Website	nij.ojp.gov

U.S. Department of Homeland Security (DHS) / FEMA Grant Programs

FEMA Homeland Security Grant Program (HSGP)

HSGP funds may support mDL reader technology when framed around emergency preparedness, interoperability, or information-sharing objectives. The Urban Area Security Initiative (UASI) component is most applicable for larger metropolitan agencies. Frame the grant narrative around mDL integration with CAD/RMS as an identity verification and information-sharing capability that supports incident response and jurisdictional interoperability.

Detail	Information
Administering Agency	FEMA, DHS; distributed through State Administrative Agencies (SAAs)
Grant Type	Formula sub-award (SHSP and UASI); no match requirement
LETPA Requirement	A percentage of SHSP and UASI funds must support Law Enforcement Terrorism Prevention Activities (LETPA) — the specific percentage is set annually in the NOFO. mDL identity authentication investments may qualify.
mDL Nexus	Digital identity authentication is a homeland security capability. mDL readers that cryptographically verify government-issued credentials at point of contact directly support HSGP's prevention and identity assurance missions. Frame as 'identity verification and authentication technology' rather than 'driver's license reader.'
Access Path	Apply through your state's designated State Administrative Agency (SAA). UASI funds are limited to eligible high-risk urban areas as determined annually by FEMA. Contact your state homeland security office for state-specific solicitation cycles and deadlines.
Website	fema.gov/grants/preparedness/homeland-security

State and Local Cybersecurity Grant Program (SLCGP)

CISA's SLCGP funds cybersecurity improvements at state and local levels. The CJIS-compliant software infrastructure and secure data handling components of mDL integration may qualify, particularly for agencies upgrading reader software and CAD/RMS integration middleware.

Detail	Information
Administering Agency	CISA, DHS; distributed through state cybersecurity offices
Grant Type	Formula sub-award; state must have an approved Cybersecurity Plan
mDL Nexus	The cryptographic Public Key Infrastructure (PKI) that enables mDL trust chain validation — certificate authority integration, AAMVA Digital Trust Service connectivity, FIPS 140-2 compliant encryption — is a cybersecurity infrastructure investment. Agencies upgrading CAD/RMS middleware for mDL integration may be able to frame PKI and secure communications components under SLCGP.
Practical Application	SLCGP is best suited for the software infrastructure and cybersecurity compliance components of mDL deployment (CJIS ISA requirements, encrypted data handling, audit logging) rather than for reader hardware procurement.
Access Path	Contact your state's designated cybersecurity office or SAA. States must develop and maintain an approved Cybersecurity Plan to access SLCGP funds.
Website	fema.gov/grants/preparedness/state-local-cybersecurity-grant-program

U.S. Department of Transportation — FMCSA Grant Programs

The Federal Motor Carrier Safety Administration (FMCSA) administers grant programs specifically targeting the safety and enforcement of commercial motor vehicles (CMVs). For agencies with motor carrier enforcement responsibilities, mDL reader technology has a direct and compelling nexus to FMCSA's mission: commercial driver's license (CDL) holders present mDLs, and officers who can verify those credentials quickly and accurately — and port the data directly into inspection reports — improve both enforcement efficiency and data quality. Agencies should engage their state MCSAP lead agency to explore these channels.

Motor Carrier Safety Assistance Program (MCSAP) — Formula Grant

MCSAP is FMCSA's largest grant program and the foundational formula funding stream for state commercial vehicle enforcement activities. MCSAP funds flow to designated state MCSAP lead agencies (typically state police or DOT enforcement divisions), which may sub-award or coordinate with local agencies.

Detail	Information
Administering Agency	FMCSA; distributed to state MCSAP lead agencies (typically state police or DOT)
Grant Type	Formula (non-competitive)
Eligible Uses for mDL	CMV inspection technology, enforcement officer equipment, safety data improvement, traffic enforcement supporting CMV safety
Match Requirement	Varies; consult the current MCSAP Comprehensive Policy (MCP)
mDL Nexus	CDL holders present mDLs; mDL readers speed up inspection initiation and allow auto-population of roadside inspection reports, reducing transcription errors in MCMIS data
Application Path	Through your state MCSAP lead agency and the Commercial Vehicle Safety Plan (CVSP) process. Contact your FMCSA Division Office to identify your state's lead agency and current CVSP cycle.
Local Agency Access	Local law enforcement agencies generally cannot apply directly for MCSAP formula funds. However, state MCSAP lead agencies can sub-award, coordinate, or provide equipment to local agencies engaged in CMV enforcement. Agencies with active truck enforcement programs should engage their state police CMV/motor carrier division.
Website	fmcsa.dot.gov/grants ai.fmcsa.dot.gov/Grants/MCSAP.aspx

High Priority — Innovative Technology Deployment (HP-ITD) Grant

The HP-ITD program is FMCSA's dedicated grant for deploying intelligent transportation system applications that advance CMV enforcement. It directly funds technology that automates data collection, links federal and state motor carrier information systems, and reduces costs associated with CMV operations and regulatory compliance.

Detail	Information
Administering Agency	FMCSA (discretionary/competitive)
Eligible Applicants	States, D.C., Puerto Rico, and U.S. territories ONLY. Applicant must have an FMCSA-approved Program Plan/Top Level Design

	(PP/TLD). If not the lead ITD agency, an MOU with the lead agency is required.
Eligible Uses for mDL	Deployment of technology to automate CMV enforcement data collection and display; linking federal motor carrier safety information systems with state CMV systems; improving safety and productivity of commercial drivers; electronic inspection capabilities including CMV driver authentication
mDL Nexus	mDL readers that auto-populate roadside inspection reports, link to MCMIS/SAFER, and verify CDL validity at point of contact fit squarely within HP-ITD's mission of 'simplifying enforcement operations by automating data collection, transfer, and display'
Application Path	Apply on grants.gov ; requires approved PP/TLD. Contact: FMCSAHPGRANTS@dot.gov
Website	ai.fmcsa.dot.gov/Grants/ITD.aspx

High Priority — Commercial Motor Vehicle Safety (HP-CMV) Grant

The HP-CMV program funds CMV safety activities including new technology demonstrations, safety data improvement projects, and targeting unsafe driving in high-risk corridors. Unlike HP-ITD, HP-CMV is open to a broader range of eligible applicants including local governments and nonprofits.

Detail	Information
Administering Agency	FMCSA (discretionary/competitive)
Eligible Applicants	State government agencies; local governments (county, city, township, special district); federally recognized tribal governments; nonprofits with 501(c)(3) status. For-profit organizations are NOT eligible.
Eligible Uses for mDL	Demonstrating new technologies to improve CMV safety, safety data improvement, targeting unsafe driving in high-risk crash corridors, public education on CMV safety
mDL Nexus	mDL reader pilots that improve CDL verification accuracy at CMV inspections, reduce MCMIS data entry errors, or demonstrate technology use in high-risk corridor truck enforcement
Application Path	Annual NOFO released typically in Q1 on grants.gov . Review current NOFO for specific eligible priorities.
Website	ai.fmcsa.dot.gov/Grants/HighPriority.aspx

High Priority — Enforcement Training and Support (HP-ETS) Grant

⚠ HP-ETS Eligibility — Nonprofit Organizations Only

HP-ETS is restricted EXCLUSIVELY to 501(c)(3) nonprofit organizations with expertise in training non-federal employees. Government agencies — including state police, local law enforcement, and state DOTs — are NOT eligible to apply directly. Law enforcement agencies seeking HP-ETS-funded mDL training must partner with an eligible nonprofit (e.g., CVSA, IACP, or a state law enforcement training academy organized as a nonprofit) to serve as the applicant; the LE agency becomes the training recipient.

Detail	Information
Administering Agency	FMCSA (discretionary, cooperative agreement)
Eligible Applicants	EXCLUSIVELY 501(c)(3) nonprofit organizations with: (1) expertise in conducting training programs for non-federal employees, and (2) ability to reach a target population of CMV safety enforcement and compliance employees. Government agencies cannot apply directly.
Eligible Uses	Development and delivery of training for non-federal personnel who conduct CMV enforcement activities; training curriculum development; instructor training
mDL Pathway for LE Agencies	Identify an eligible nonprofit training partner early. The nonprofit applies and receives the award; your agency is the training recipient. Suitable partners may include CVSA, IACP, or accredited nonprofit law enforcement training academies.
Website	ai.fmcsa.dot.gov/Grants/HighPriority.aspx

✓ Grant Writing Tip — FMCSA Programs

FMCSA's NOFOs prioritize safety data improvement and new technology demonstrations. For mDL proposals, frame the project around: (1) reducing transcription errors in MCMIS inspection and crash data by using mDL-sourced identity data; (2) automating CDL status verification at point of contact; and (3) linking mDL reader output to existing state CMV information systems. Cite FMCSA's stated goal of 'simplifying enforcement operations by automating data collection, transfer, and display.' Engage your FMCSA Division Office early — they can confirm PP/TLD status and advise on project alignment.

U.S. Department of Transportation — NHTSA Highway Safety Grant Programs

The National Highway Traffic Safety Administration (NHTSA) administers formula grant programs — primarily Section 402 and Section 405 — that flow through State Highway Safety Offices (SHSOs), typically housed within a state's Governor's Office of Highway Safety or Department of Transportation. These are not competitive grants applied for directly by local

agencies; instead, local law enforcement agencies access this funding through sub-award processes administered by the SHSO.

NHTSA Section 402 — State and Community Highway Safety Grant Program

Detail	Information
Administering Agency	NHTSA at federal level; State Highway Safety Offices (SHSOs) / Governors' Highway Safety Offices at state level
Grant Type	Formula (non-competitive; flows through state to local sub-recipients). 80% federal / 20% state match required. At least 40% of funds must be spent by or for the benefit of local governments.
Eligible Uses for mDL	Equipment and technology supporting traffic enforcement; e-citation system integration; crash report quality improvements; officer training on traffic enforcement technology
mDL Nexus	mDL-integrated e-citation systems that auto-populate citation fields reduce officer time and citation errors. mDL-sourced crash report data improves MMUCC compliance and crash data quality.
Access Path	Contact your state Governor's Highway Safety Office or SHSO. Request inclusion of mDL reader technology in the state Highway Safety Plan (HSP) as an eligible sub-recipient project. State HSP applications to NHTSA are due August 1 annually. The Governors Highway Safety Association (GHSA) maintains a directory of all state SHSOs at ghsa.org .
Website	nhtsa.gov/highway-safety-grants-program

NHTSA Section 405(c) — State Traffic Safety Information System Improvements

Section 405(c) is the most directly applicable NHTSA funding source for agencies seeking to improve crash data quality through mDL integration. This incentive grant program supports state programs that improve the timeliness, accuracy, completeness, uniformity, integration, and accessibility of state safety data. These are precisely the data quality dimensions improved when mDL-sourced identity data auto-populates crash reports, eliminating transcription errors.

Detail	Information
Administering Agency	NHTSA; administered by state SHSOs through state Traffic Records Coordinating Committees (TRCCs)
Grant Type	Incentive formula grant. State must demonstrate quantifiable improvement in traffic records quality. 80/20 federal/state match required.

Eligible Uses for mDL	Equipment to upgrade crash data collection systems; adoption of electronic crash reporting by law enforcement; improving compatibility and interoperability of traffic safety databases; aligning crash data with MMUCC; traffic data quality improvement research and training
mDL Nexus	mDL readers integrated with e-crash report systems directly address 405(c)'s mandate to improve crash data accuracy and timeliness by eliminating manual identity data transcription. Framing mDL integration as a crash data quality improvement positions it squarely within 405(c) eligibility.
Eligibility Requirement	State must have an active TRCC, a designated traffic records coordinator, and a current Traffic Records Strategic Plan. The project must demonstrably advance the plan's goals for one or more of the six data quality attributes.
Access Path	Contact your state TRCC Coordinator (often housed in the state SHSO or DOT). Request inclusion of mDL-integrated crash reporting in the state's annual Traffic Records Strategic Plan project solicitation.
Website	nhtsa.gov/data/traffic-records transportation.gov/government/traffic-records

✓ Grant Writing Tip — NHTSA Section 405(c)

When developing a 405(c) project proposal, ground the application in NHTSA's six crash data quality attributes: timeliness, accuracy, completeness, uniformity, integration, and accessibility. Document current baseline error rates in crash report identity fields (name misspellings, incorrect DL numbers), and propose mDL integration as a technology solution with measurable improvement targets. NHTSA traffic records assessments showing weakness in crash data accuracy are strong supporting justification. Reference the MMUCC 6th Edition (DOT HS 813 525a, 2025) and NHTSA Traffic Records Data Quality Management Guide (DOT HS 813 544, 2024) as the authoritative design standards.

NHTSA BIL — State Electronic Crash Data Collection Program

Section 24108(d)(2) of the Bipartisan Infrastructure Law created a discretionary grant program to support states in upgrading crash data systems for electronic data collection and transfer to NHTSA. Its explicit mandate supports 'adoption of electronic crash reporting by law enforcement agencies' and 'increasing alignment of State crash data with MMUCC' — directly encompassing mDL-integrated crash reporting. Agencies should monitor NHTSA for NOFOs under this

program and coordinate with their state SHSO to position mDL integration within state-level applications.

State and Local Funding Sources

Federal formula programs flow through state agencies that in turn sub-award to local law enforcement. Understanding the state-level access points — and building relationships with them — is as important as understanding the federal programs themselves. The specific agency names and contact points will vary by jurisdiction; the categories below reflect the typical structure found across U.S. states and Canadian provinces.

Source	Description and Access Path
State Administering Agency (SAA) — JAG Pass-Through	State SAAs distribute federal JAG formula funds and may operate their own technology grant programs for local law enforcement. Contact your state's designated SAA to identify current solicitation cycles and deadlines. (Example: In many states this is the state attorney general's office, department of public safety, or a state criminal justice agency.)
State SHSO/GHSO — NHTSA Sub-Grants	State highway safety offices sub-award Section 402 and 405(c) funds through annual solicitations. Contact your state SHSO to request inclusion in the next solicitation cycle and ensure your project concept aligns with the state's Highway Safety Plan and Traffic Records Strategic Plan.
State MCSAP Lead Agency	State MCSAP lead agencies (typically the state police or a state DOT enforcement division) may provide equipment, training, or sub-awards to local agencies engaged in CMV enforcement activities. Agencies with active truck enforcement programs should engage their state's MCSAP lead agency.
Asset Forfeiture Funds	Where permitted by state law and agency policy, asset forfeiture proceeds may fund equipment and technology acquisitions. Verify applicable state statutes and agency policy before proceeding.
General Fund Technology Refresh Budgets	The most sustainable long-term approach — incorporate mDL capability into planned equipment refresh cycles funded through normal capital budget processes. Most durable funding path for ongoing sustainment.
State Legislative Appropriations	Direct appropriations through the annual state budget process. Agencies with strong legislative relationships can seek line-item funding for technology modernization. Requires early engagement with legislative staff, typically several months before the legislative session begins. Multi-agency or statewide consortium requests carry more weight.
Regional / Multi-Agency Partnerships	Agencies sharing CAD infrastructure or operating in a regional traffic safety corridor can pool procurement and share integration

development costs. Regional consortia also strengthen competitive grant applications — higher per-award impacts score better.

Congressional Appropriations Earmarks

Congressional directed spending (earmarks) represent one of the highest-value and least-utilized funding strategies for law enforcement technology. They are not widely understood by agency grant staff but are actively accessible through the right engagement strategy.

Beyond the COPS TEP program (which is itself funded by earmarks), individual agencies can seek congressional directed spending across multiple appropriations bills. Members of Congress in both the House and Senate can request — and frequently receive — specific allocations for law enforcement technology within their home districts and states.

How Congressional Earmarks Work for LE Technology

- Member Directed Spending requests are submitted annually by Members of Congress (both House and Senate) to their respective Appropriations Committees, typically in January–February for the fiscal year beginning October 1.
- Agencies must provide their congressional representative with a project description, cost estimate, and justification before the request deadline. Your agency's government affairs staff or your congressional delegation office are the starting points.
- For law enforcement technology, the most relevant appropriations bills are Commerce, Justice, Science (CJS — covers DOJ/COPS) and Transportation, Housing and Urban Development (THUD — covers DOT/NHTSA/FMCSA).
- Multi-agency or statewide requests are more competitive. A consortium of agencies sharing mDL reader infrastructure is more compelling to a congressional office than a single-agency request.
- Earmarks require public disclosure — the requesting Member's name, the recipient agency, and the dollar amount are public record.

✓ Strategic Tip — Congressional Engagement

Start conversations with your congressional delegation offices well before the next request deadline. Provide a one-page project summary including: agency name, project description, total cost, and federal amount requested. Reference the growing prevalence of mDL adoption nationally and your state's current or imminent mDL implementation status. Frame the investment as supporting officer safety (reduced time at roadside) and data quality (elimination of transcription errors affecting criminal hit rates). Your state law enforcement association can amplify multi-agency requests.

Cooperative Purchasing Programs

Cooperative purchasing contracts allow agencies to acquire technology without a full competitive procurement. These are particularly useful for accelerating initial deployment while longer-term integrated procurement is planned.

Contract Vehicle	Description	Website
GSA Multiple Award Schedules (MAS)	Federal and eligible state/local agencies. Search Schedule 84 (Law Enforcement, Security, and CBRN Equipment) and Schedule 70 (IT) for identity verification and public safety technology. Most commonly used cooperative contract vehicle.	gsa.gov
NASPO ValuePoint	National cooperative contracts from the National Association of State Procurement Officials; open to state and local agencies in participating states. Check for public safety and technology categories.	naspovaluepoint.org
Sourcewell	Cooperative purchasing for government and education; check for public safety and technology contracts.	sourcewell-mn.gov
State Master Contracts	Most states maintain statewide contracts for law enforcement technology. Contact your state's purchasing or procurement office to identify applicable contracts for reader hardware and software.	Contact state purchasing office

Vendor Financing & OpEx Models

When upfront capital funding is unavailable or grant timelines are too long, OpEx models offered by technology vendors can bridge the gap:

Model	Description
Device-as-a-Service (DaaS)	Monthly per-device fee covering hardware, software, maintenance, and refresh. Converts CapEx to a predictable operating expense.

	Most useful for agencies with annual operating budget flexibility but no capital budget.
Software-as-a-Service (SaaS)	Monthly per-officer or per-agency subscription for reader software, including updates and support. Allows hardware to be purchased via grant while software is sustained through operating budget.
Bundled Device + Data Plans	Government-rate carrier bundles including device and cellular data at reduced monthly cost. Note: cellular data is not required for mDL verification itself but is needed for CIC/NCIC queries on the same device.
Lease-to-Own	Lease arrangements that transfer ownership at end of term — combining OpEx cash flow with eventual CapEx ownership. Ensures hardware refresh at defined intervals.

Blended Funding Strategy — Practical Model

A practical approach: use JAG or FMCSA HP-CMV grant funds for initial hardware acquisition; use a SaaS subscription for the reader software and ongoing updates; and coordinate with your state SHSO on 405(c) funding for crash-report integration development. This spreads cost across three funding sources aligned to three distinct agency missions — criminal justice, CMV safety, and crash data quality — and reduces dependency on any single grant program or budget cycle.

Grant Writing Tips for mDL Technology

General Tips (All Programs)

- Clearly articulate the operational problem: officers encountering mDLs without tools to read them; manual data entry errors causing missed criminal hits on NCIC queries and lower data quality on reports; re-entry time that reduces patrol capacity.
- Quantify where possible: number of officers receiving readers, estimated time savings per stop, projected reduction in data entry errors. Even rough estimates grounded in documented baselines are valuable.
- Reference AAMVA data on state mDL adoption rates to show the problem is growing — officers will encounter mDLs whether the agency is ready or not. As of early 2026, 21 states plus Puerto Rico have TSA-recognized mDL programs.
- Cite applicable state legislation on mDL acceptance or reader deployment to establish urgency and policy alignment.
- Always include training costs — they are allowable under virtually all programs listed in this document.
- Address Total Cost of Ownership (TCO): include software license renewals, certificate authority subscription fees, personnel training for new hires, and hardware refresh in the grant budget narrative and sustainment plan.

- Consider consortia applications: a multi-agency submission covering a regional corridor or statewide deployment scores higher on impact metrics and broadens congressional/administrative support.

FMCSA-Specific Framing

- Emphasize the CDL/mDL connection: commercial drivers already have mDLs, and inspectors who can verify CDL credentials instantly improve both enforcement efficiency and MCMIS data accuracy.
- Use FMCSA's own HP-ITD language: cite 'simplifying enforcement operations by automating data collection, transfer, and display' as the project goal.
- For HP-CMV: document baseline MCMIS data quality issues attributable to manual transcription of CDL identity data and propose mDL integration as the measured improvement.
- For HP-ETS: identify a 501(c)(3) nonprofit training partner early. The nonprofit must be the applicant; your agency is the training recipient.

NHTSA 405(c) / Traffic Records Framing

- Ground the proposal in NHTSA's six crash data quality attributes: timeliness, accuracy, completeness, uniformity, integration, and accessibility.
- Document current error rates in crash report identity fields (name errors, incorrect DL numbers) as baseline metrics to improve.
- Reference MMUCC 6th Edition data element requirements and show how mDL-sourced data achieves higher MMUCC compliance than manual entry.
- Engage your state TRCC Coordinator early — 405(c) projects must appear in the state Traffic Records Strategic Plan before they can be funded.

Grant Program Sequencing Strategy

Sophisticated agencies pursue a deliberate sequencing strategy rather than applying to programs opportunistically:

- **Phase 1 — Pilot (Year 1):** Apply for a NIJ demonstration grant or use JAG funds for a limited pilot deployment. Document baseline metrics (stop time, error rates, officer feedback) rigorously.
- **Phase 2 — Scale (Years 1–2):** Use pilot performance data to support competitive grant applications (HP-CMV, BWC Implementation). Stronger data = stronger narrative = higher scores.
- **Phase 3 — Sustain:** Incorporate the technology into annual JAG formula requests and NHTSA sub-grant cycles. Transition software costs to SaaS/operating budget. Engage legislature for ongoing capital refresh.

Funding Program Quick Reference

Program	Agency	Best mDL Use Case	Type	Local Access Path
JAG (Edward Byrne)	DOJ/BJA	General LE reader hardware & software; training	Formula + Competitive	Via state SAA
COPS TEP	DOJ/COPS	LE technology & equipment	Invitational Only — JES earmark	Must be named in Congressional JES — engage your delegation
CPD Microgrants	DOJ/COPS	Community policing technology innovation	Competitive	Direct application (justgrants.usdoj.gov)
BWC Policy & Implementation	DOJ/BJA	mDL as digital evidence management	Competitive	Direct application (justgrants.usdoj.gov)
NIJ Demonstration	DOJ/NIJ	mDL pilot site & evaluation	Competitive	Direct application (nij.ojp.gov)
FEMA HSGP / UASI	DHS/FEMA	Interoperability & identity auth framing	Formula (sub-award)	Via state SAA / state homeland security office
SLCGP	DHS/CISA	PKI / CJIS-compliant software infrastructure	Formula (sub-award)	Via state cybersecurity office
MCSAP	USDOT/FMCSA	CMV inspection technology & enforcement	Formula (sub-award)	Via state MCSAP lead agency
HP-ITD	USDOT/FMCSA	CMV enforcement tech & MCMIS/SAFER data links	Competitive	States only (requires PP/TLD)
HP-CMV	USDOT/FMCSA	New CMV technology demos, safety data improvement	Competitive	Direct (states, local govts, nonprofits)
HP-ETS	USDOT/FMCSA	CMV enforcement officer training	Competitive — nonprofits ONLY	Partner with 501(c)(3) nonprofit applicant

NHTSA Section 402	USDOT/NHTSA	e-Citation & traffic enforcement technology	Formula (sub-award)	Via state SHSO/GHSO
NHTSA Section 405(c)	USDOT/NHTSA	Crash data quality & electronic crash reporting	Incentive formula (sub-award)	Via state TRCC / SHSO
BIL State Electronic Data	USDOT/NHTSA	State crash data system modernization	Discretionary	Via state SHSO
Congressional Earmarks	Congress / DOJ or DOT	Large-scale or statewide mDL technology deployments	Member-directed spending	Engage House & Senate offices (Jan–Feb deadline)

Acronym Glossary

Acronym	Definition
AAMVA	American Association of Motor Vehicle Administrators
BJA	Bureau of Justice Assistance (U.S. DOJ)
BIL	Bipartisan Infrastructure Law (Infrastructure Investment and Jobs Act, P.L. 117-58)
BLE	Bluetooth Low Energy
BWC	Body-Worn Camera
BWCPIP	Body-Worn Camera Policy and Implementation Program (BJA)
CAD	Computer-Aided Dispatch
CapEx	Capital Expenditure
CDL	Commercial Driver's License
CJIS	Criminal Justice Information Services (FBI)
CJS	Commerce, Justice, Science (Congressional appropriations bill)
CMV	Commercial Motor Vehicle
COPS	Office of Community Oriented Policing Services (U.S. DOJ)
CPD	Community Policing Development

CVSA	Commercial Vehicle Safety Alliance
CVSP	Commercial Vehicle Safety Plan
DaaS	Device-as-a-Service
DHS	U.S. Department of Homeland Security
DOJ	U.S. Department of Justice
DOT	Department of Transportation (U.S. or state level)
DTS	AAMVA Digital Trust Service
FBR	Field-Based Reporting
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FMCSA	Federal Motor Carrier Safety Administration
GHSO	Governor's Highway Safety Office
HP-CMV	High Priority — Commercial Motor Vehicle Safety Grant (FMCSA)
HP-ETS	High Priority — Enforcement Training and Support Grant (FMCSA)
HP-ITD	High Priority — Innovative Technology Deployment Grant (FMCSA)
HSP	Highway Safety Plan
HSGP	Homeland Security Grant Program (FEMA)
IACP	International Association of Chiefs of Police
ISA	Information Security Agreement (CJIS context)
JAG	Edward Byrne Memorial Justice Assistance Grant
JES	Joint Explanatory Statement (Congressional appropriations)
LETPA	Law Enforcement Terrorism Prevention Activities
MCMIS	Motor Carrier Management Information System (FMCSA)
MCSAP	Motor Carrier Safety Assistance Program
mDL	Mobile Driver License
MMUCC	Model Minimum Uniform Crash Criteria
MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NFC	Near-Field Communication
NHTSA	National Highway Traffic Safety Administration
NIJ	National Institute of Justice

NOFO	Notice of Funding Opportunity
OpEx	Operating Expenditure
PKI	Public Key Infrastructure
PP/TLD	Program Plan / Top Level Design (FMCSA HP-ITD eligibility requirement)
RMS	Records Management System
SAA	State Administering Agency
SAFER	Safety and Fitness Electronic Records (FMCSA)
SaaS	Software-as-a-Service
SHSP	State Homeland Security Program
SHSO	State Highway Safety Office
SLCGP	State and Local Cybersecurity Grant Program
TCO	Total Cost of Ownership
TEP	Technology and Equipment Program (COPS Office)
THUD	Transportation, Housing and Urban Development (Congressional appropriations bill)
TRCC	Traffic Records Coordinating Committee
UASI	Urban Area Security Initiative
USDOT	U.S. Department of Transportation

Related Toolkit Documents

Document	Content
DOC-01	Standards Overview — ISO/IEC 18013-5 & 18013-7, AAMVA guidelines, national mDL landscape
DOC-02	Hardware & Software Requirements — cost components to budget in grant applications; CJIS compliance baseline
DOC-04	Operational Workflows — use case documentation to support grant narratives and needs assessments
DOC-05	Procurement Considerations & Strategy — solicitation requirements and contract framework
DOC-07	Legal & Privacy Considerations — state law, data retention, CJIS, and Fourth Amendment

This document is a component of the AAMVA Law Enforcement mDL Toolkit. For questions or corrections, contact AAMVA at aamva.org.

LAW ENFORCEMENT mDL TOOLKIT
DOC-07

Legal & Privacy Considerations

State Acceptance Law, Data Minimization, CJIS Compliance, and Fourth Amendment Guidance

Audience	Legal Counsel, Command Staff, Policy Officers
Purpose	Addresses the legal and privacy landscape governing law enforcement use of mDL technology, including state acceptance law variability, data minimization requirements, CJIS Security Policy obligations, data retention policy guidance, and Fourth Amendment considerations. This document should be reviewed with agency legal counsel before deployment.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

Legal Counsel Review Required

This document provides general guidance, not legal advice. Agency legal counsel must review all aspects of mDL deployment — including policy development, data retention schedules, procurement contracts, and officer training content — before deployment. State law varies significantly, and the legal landscape is evolving.

State Acceptance Law

Law enforcement authority to accept mDLs as valid credentials is not uniform across states, and the legal landscape is changing rapidly. Agencies must understand their jurisdiction's current legal posture before deploying mDL reader technology.

Legal Posture	Description & Agency Action Required
Mandatory Acceptance Law	Some states (e.g., Georgia via HB 296, 2025) have enacted laws requiring officers to accept mDLs when equipped with a reader, and mandating agency-wide reader deployment by a specified date. Agencies in these states have a statutory obligation to deploy. Confirm effective date and equipment requirements.
Permissive / Authorizing Law	Some states have enacted laws authorizing — but not requiring — officers to accept mDLs. Officers may, but are not required to, accept an mDL as valid identification. Agency policy should clarify officer obligations when a driver presents an mDL.
No Specific Legislation	Many states have no specific mDL legislation. In these jurisdictions, officers may still encounter mDLs issued from other jurisdictions. Because the mDL is an extension of the physical, legitimately-issued driver license or ID card, agencies with mDL verification capabilities are likely permitted to accept the mDL. Engage agency legal counsel and the state DMV for a formal determination.
Adverse or Restrictive Legislation	A small number of jurisdictions may have passed laws restricting relying parties from requiring digital identity presentation. While this should not hinder acceptance of mDL, legal counsel must review before any mDL deployment.

AAMVA's mDL Model Legislation provides a template for jurisdictions seeking to enact clear mDL acceptance law. Agencies in states without clear acceptance authority should engage their legislative affairs contacts and DMV to advocate for legislative clarity.

Physical Credential Requirement Remains

Regardless of state mDL acceptance law, most states currently require drivers to carry their physical credential when operating a motor vehicle. Though mDLs present the same data — from the same data source — as physical driver licenses and ID cards, most relying parties do not yet have the capability of reading and authenticating mDLs. Officers should continue

to request physical credentials when an mDL cannot be verified or when the encounter requires physical credential examination.

Data Minimization and Selective Disclosure

ISO/IEC 18013-5 is built on the principle that relying parties (including law enforcement) should request only the data elements necessary for the specific transaction. AAMVA's Model Legislation codifies this principle, providing that relying parties shall only request data elements necessary to complete the transaction for which the data is being requested.

In the case of law enforcement encounters, it is generally understood Law Enforcement mDL readers will request all available mDL data.

Data Retention Policy

Generally, mDL data should be handled in the manner and retained for the same periods as is data obtained from physical drivers. However, because the proliferation of digital identity credentials has introduced new questions and concerns regarding data privacy, agencies may wish to consider developing and adopting a formal data retention policy governing mDL transaction data before deploying reader technology. Policy considerations should address:

- **Retention Period:** How long is mDL transaction data retained in the CAD/RMS? Is it tied to the incident record, or maintained separately?
- **Non-Incident Retention:** Is mDL data that does not result in a citation, report, or arrest retained at all? If so, under what legal authority, and for how long?
- **Local Device Retention:** Does the reader application retain transaction data locally on the officer's device? If so, confirm the retention period and purge mechanism with the vendor.
- **Compliance with State Records Law:** Retention schedules must comply with applicable state public records retention law. Confirm that mDL transaction data is classified under the appropriate records retention schedule.
- **CJIS Compliance:** Any mDL transaction data commingled with Criminal Justice Information is subject to FBI CJIS Security Policy retention and destruction requirements.

CJIS Security Policy

The FBI Criminal Justice Information Services (CJIS) Security Policy applies to any system that stores, transmits, or interfaces with Criminal Justice Information (CJI). Because mDL data will routinely be used to initiate NCIC/CIC queries — and the results of those queries are CJI — the mDL reader and its integration software may be subject to CJIS requirements.

Key CJIS requirements for mDL deployments:

- **Encryption:** All CJI in transit must be encrypted using FIPS 140-2 compliant algorithms. Verify with all vendors.

- **Multi-Factor Authentication:** Advanced authentication is required for access to systems containing CJI.
- **Audit Logging:** All access to CJI must be logged. Reader software integrated with CJI systems must maintain compliant audit logs.
- **Vendor ISA:** All vendors with access to CJI data must execute a CJIS Information Security Agreement (ISA). This is a mandatory contract requirement.
- **Personnel Security:** Vendor employees with unescorted access to CJI systems must have completed required background checks.

Fourth Amendment Considerations

Agency legal counsel should review the intersection of mDL technology with Fourth Amendment jurisprudence. The following areas warrant specific attention:

Data Minimization and Scope of Request

Requesting mDL data elements beyond what is legally required for a given encounter may raise Fourth Amendment questions. Officers and agencies should establish clear policy on what data elements may be requested for each encounter type and ensure reader applications are configured accordingly.

Plain View During mDL Engagement

During NFC or QR engagement, the officer's proximity to the holder's device may raise questions about whether the contents of the phone visible during the engagement are subject to plain view doctrine. Officers should not examine phone contents beyond what is necessary to initiate the mDL session. Under no circumstances should an officer touch or otherwise handle a subject's mDL device (i.e. mobile phone) solely for the purpose of reading or authenticating an mDL.

Long-Term Surveillance Risk

The ISO/IEC 18013-5 standard's non-tracking design — where no central server logs the transaction — is a significant privacy protection. Agencies should avoid implementing supplemental logging systems that recreate the surveillance risk the standard was designed to prevent, as such systems could be challenged as warrantless tracking.

Policy Development Checklist

Before deploying mDL reader technology, agencies should consider developing policies addressing the following:

- ☐ Officer authority to accept mDLs — defined by reference to applicable state law
- ☐ Data elements authorized for request in each encounter type
- ☐ mDL transaction data retention schedule — compliant with state records law and CJIS Security Policy

- ☐ Procedures when mDL cannot be verified — fallback to physical credential
- ☐ Prohibition on accessing phone contents beyond mDL session initiation
- ☐ Vendor CJIS ISA requirement — standard contract provision
- ☐ Officer training requirement on legal and privacy obligations

Related Toolkit Documents

- **DOC-01:** Standards Overview — privacy protections built into ISO/IEC 18013-5
- **DOC-05:** Procurement Considerations — CJIS ISA and data ownership contract requirements
- **DOC-08:** Training Plan Framework — officer training on legal and privacy obligations

LAW ENFORCEMENT mDL TOOLKIT
DOC-08

Training Plan Framework

Curriculum Outline, Delivery Formats, and Competency Standards for Agency mDL Training

Audience	Training Officers, Field Training Officers, Supervisors, Command Staff
Purpose	Provides a structured framework for developing and delivering agency-wide mDL training programs, including audience-specific curriculum outlines, recommended delivery formats, competency standards, and a train-the-trainer model.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

Customize Before Use

This document provides a framework, not a finished training program. Each agency must adapt this content to reflect its specific reader application, CAD/FBR integration setup, applicable state law, and agency policy. Before finalizing training content, confirm all technical procedures with your reader vendor and all legal content with agency counsel.

Training Program Overview

A complete agency mDL training program addresses four distinct audiences with different informational needs:

Audience	Primary Need	Training Modules
Patrol Officers	How to use the reader in the field; what to do when it doesn't work	Modules 1–5 (full curriculum)
Supervisors / Sergeants	Officer oversight, policy interpretation, and escalation procedures	Modules 1–5 plus Supervisor Supplement
Technology / IT Staff	Device deployment, integration management, CJIS compliance	Modules 1, 3, and IT Technical Supplement
Command Staff	Strategic context, legal landscape, and policy requirements	Module 1 and Executive Briefing (30 min)

Training Curriculum — Module Outlines

Module 1: What Is an mDL? (30 min — All Personnel)

This foundational module is required for all agency personnel. It provides the conceptual framework all other modules build on.

- **Learning Objectives:** Personnel will be able to explain what an mDL is, how it differs from a photo of a license, and why ISO/IEC 18013-5 compliance matters.
- What mDL is — and is not (not a photo, not a barcode scan, not a visual display)
- The three parties: Holder, Issuing Authority, and Verifier
- How cryptographic signing works in plain language (DMV signs the data; reader checks the signature)
- Overview of mDL wallet implementations
- Current state, province, and territory adoption — which jurisdictions have mDLs your officers will encounter
- Legal status in your jurisdiction — what the law says about accepting mDLs

Module 2: Field Verification — Using the Reader (60 min — Patrol + Supervisors)

Hands-on skill development module. Must include practical demonstration and scenario-based exercise using the agency's actual reader application.

- **Learning Objectives:** Officers will be able to successfully initiate and complete an mDL verification session using the agency's reader app, compare the returned photo to the holder, and interpret the displayed validity information.
- Opening and preparing the reader application
- QR code engagement — step-by-step demonstration
- NFC engagement — step-by-step demonstration
- Interpreting the holder's consent screen — what the holder sees
- Reading the reader's output — what valid looks like, what an alert looks like
- Photo comparison — how to compare the mDL portrait to the person in front of you
- Hands-on exercise: Each officer completes a minimum of 3 successful verification sessions

Module 3: Workflow Integration — Data Use and Reporting (45 min — Patrol + Supervisors, Technical Support)

Focuses on the downstream use of mDL data — the primary value driver of the technology.

- **Learning Objectives:** Officers will be able to transfer mDL data to their CAD/FBR system and confirm auto-population of reports, citations, and query fields.
- How mDL data flows to your agency's specific CAD/FBR system
- Confirming auto-population of report and citation fields
- Submitting a CIC/NCIC query using mDL-sourced DL number
- e-Citation completion using mDL data
- Crash report and arrest report field population
- Hands-on exercise: Complete a simulated traffic stop from mDL scan through e-citation issuance

Module 4: Failure Scenarios and Fallback Procedures (30 min — Patrol + Supervisors)

Prepares officers for real-world conditions where mDL verification does not work as expected.

- **Learning Objectives:** Officers will correctly identify and apply the appropriate response for every common failure scenario, including applicable legal obligations under state law and agency policy.
- Holder's device has no battery or is damaged — request physical credential; follow agency procedures and applicable state law
- Reader cannot establish a session — request physical credential; report failure to technology contact

- Holder declines consent — request physical credential; follow standard no-ID procedures if no credential is produced
- Reader displays authentication failure or warning — do not treat as valid; follow agency policy
- Out-of-state or non-ISO/IEC 18013-5 digital credentials — reader may not authenticate; request physical credential
- Holder claims to have an mDL but app is not working — request physical credential; follow agency procedures
- Scenario exercise: Practice each failure scenario with appropriate response

Module 5: Legal, Privacy, and Policy (30 min — Patrol + Supervisors)

Ensures officers understand their legal obligations and the privacy principles that govern mDL transactions.

- **Learning Objectives:** Officers will correctly state agency policy on data minimization, data retention, physical credential requirements, and applicable state law obligations.
- State/Provincial law on mDL acceptance in your jurisdiction
- Physical credential requirement — drivers are still required to carry physical licenses in most jurisdictions
- Selective disclosure — request only necessary data elements for the specific encounter
- Do not handle the holder's device
- Do not examine phone contents beyond mDL session initiation
- How mDL transaction data is retained (per agency policy)
- Reporting reader failures or policy concerns

Supervisor Supplement (45 min — Supervisors / Sergeants Only)

This supplement is required for all supervisory personnel in addition to Modules 1–5. It equips supervisors to oversee officer mDL activity, interpret policy, manage exceptions, and support the agency's ongoing deployment.

- **Learning Objectives:** Supervisors will be able to evaluate officer competency in mDL verification, apply agency policy to field exceptions, manage complaints, and serve as the first point of escalation for legal and technology issues.

Evaluating Officer Performance

- How to observe and assess officer proficiency in QR and NFC engagement
- Common officer errors: failing to confirm auto-population, skipping photo comparison, mishandling authentication failures
- Competency standards for field clearance — what passing looks like (see Competency Standards section)
- Remediation process for officers who do not meet competency standards

Policy Interpretation and Exceptions

- Applying agency data minimization policy to non-routine encounters (e.g., arrest, DUI investigation, crash)
- Supervising officer response when a holder declines consent — when to escalate
- Handling disputes at point of contact regarding mDL validity or officer authority to require a physical credential
- Jurisdiction-specific legal requirements — when state law mandates acceptance and when it does not

Complaint Handling and Escalation

- Responding to officer complaints about reader equipment or software failures
- Responding to public complaints related to mDL verification encounters
- Escalation path for unresolved legal or policy questions — agency legal advisor, state DMV liaison
- Escalation path for technology failures — agency IT/technology point of contact, vendor support

Ongoing Deployment Responsibilities

- Ensuring assigned officers maintain current training and recertification status
- Communicating policy updates, state law changes, and new reader capabilities to the team via roll call or briefings
- Monitoring for patterns of reader failure or officer non-compliance and reporting to command

Executive Briefing (30 min — Command Staff Only)

This briefing is designed for chiefs, sheriffs, deputy chiefs, and other command-level personnel. It does not require hands-on equipment training. The goal is to ensure command staff can make informed decisions about mDL deployment, respond to policy and legal questions, and provide effective leadership for the agency's adoption of this technology.

- **Learning Objectives:** Command staff will be able to describe the strategic value of mDL technology, articulate the agency's legal authority and obligations, and identify the key decisions required for successful deployment.

The mDL Landscape and Strategic Context

- What an mDL is and why it matters for law enforcement — the shift from physical to digital credentials
- Current national deployment status: which states have active mDL programs and the pace of adoption
- Why agencies that wait will be less prepared: legislative trends and officer encounter rates

- The core operational benefit: mDL data flowing directly into citations, crash reports, and queries — reduced errors, faster stops

Legal and Policy Obligations

- Your jurisdiction's current legal posture on mDL acceptance — mandatory, permissive, or silent
- Physical credential requirements — what the law currently says in your state
- Officer authority and limitations when interacting with mDL holders
- Data retention and privacy obligations — what your agency must have in policy before deploying
- CJIS Security Policy compliance — vendor and system requirements

Deployment Decisions for Command

- Procurement pathway: immediate deployment vs. integrated long-term solution — tradeoffs and timeline
- Funding options: JAG, FMCSA, NHTSA 405(c), and cooperative purchasing vehicles
- Policy development requirements before go-live: data retention, officer authority, acceptable use
- Training rollout strategy: train-the-trainer model, LMS integration, and competency standards
- Metrics and accountability: how to measure successful deployment and officer readiness

Questions for Command to Resolve Before Deployment

- Has legal counsel reviewed applicable state law and confirmed officer authority to accept mDLs?
- Has a data retention policy been adopted covering mDL transaction data?
- Has the agency selected a reader solution with a documented integration path to CAD/FBR?
- Has a vendor CJIS Information Security Agreement been executed?
- Is a training and competency certification process in place before officers are deployed with readers?

Reference for Command Staff

For full detail on any of the topics above, direct command staff to the relevant toolkit documents: DOC-01 (Standards Overview), DOC-05 (Procurement), DOC-06 (Funding), and DOC-07 (Legal & Privacy Considerations).

Delivery Format Recommendations

Format	Best Used For	Notes
In-Person / Hands-On	Modules 2, 3, 4 — skill development requiring practice with actual hardware	Must use the agency's actual reader app and CAD/FBR system — no generic demos
Online / Self-Paced (LMS)	Module 1 initial delivery; Module 5 annual refresher	Build into agency LMS for annual recertification tracking
Roll Call Training	Policy updates, state law changes, new reader capabilities	Keep to 10–15 minutes; issue written roll call handout
Quick Reference Card	Field reference for engagement steps and failure procedures	Laminated card for vest/belt/dash; QR code to refresher video
Video Demonstration	Module 2 walkthrough; failure scenario reference	Short-form (5–10 min); hosted on agency intranet or LMS
Briefing / Presentation	Executive Briefing for command staff	30 min; slide-supported; delivered by training officer or agency technology lead
Train-the-Trainer	Multiplying instructor capacity for agency-wide rollout	Certify 1 trainer per 20–30 officers; require annual recertification

Competency Standards

Officers should be assessed on the following competencies before being cleared to use mDL reader technology in the field:

- **Knowledge:** Can correctly explain what an mDL is, how it is verified, and what the reader output means.
- **Skill — QR Engagement:** Successfully completes QR-initiated mDL verification session with no coaching in at least 3 of 3 attempts.
- **Skill — NFC Engagement:** Successfully completes NFC-initiated mDL verification session with no coaching in at least 3 of 3 attempts.
- **Skill — Data Integration:** Can correctly transfer mDL data to CAD/FBR system and confirm report field population.
- **Judgment — Failure Scenarios:** Correctly identifies appropriate response — including applicable legal obligations — for each of 5 presented failure scenarios without prompting.
- **Policy:** Can correctly state agency policy on data minimization, physical credential requirements, and holder consent.

Related Toolkit Documents

- **DOC-01:** Standards Overview — foundational mDL technology content for Module 1

- **DOC-04:** Operational Workflows — step-by-step field procedures that Modules 2, 3, and 4 must cover
- **DOC-05:** Procurement Considerations & Strategy — deployment decision content for the Executive Briefing
- **DOC-06:** Funding Strategies & Opportunities — funding content for the Executive Briefing
- **DOC-07:** Legal & Privacy Considerations — legal content for Module 5 and the Executive Briefing
- **DOC-09:** mDL Officer How-To Guide — field reference to distribute to officers on completion of Module 2
- **DOC-10:** mDL FAQs for Law Enforcement — supplementary reading for officers completing initial training

LAW ENFORCEMENT mDL TOOLKIT

DOC-09

mDL Officer How-To Guide

Step-by-Step Instructions for Mobile Driver License Encounters

Audience	Patrol Officers, Field Training Officers
Purpose	A plain-language, instructional guide for patrol officers on how to verify a mobile driver license, how to use the data in citations and reports, and what to do when something does not go as expected. No technical background required.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

Know Before You Go

An mDL is a real, government-issued license — not a photo. A mobile driver license stored in a digital wallet (Apple Wallet, Google Wallet, or a state app) is a genuine credential issued by the DMV. A photo or screenshot of a license is not an mDL and cannot be verified.

You need a reader. Your agency will issue or designate an approved mDL reader app or device capable of authenticating and displaying mDL data. Make sure it is charged and ready before your shift.

You never touch the driver's phone. All data transfers wirelessly. The driver keeps their device.

The driver must approve what you receive. Before any data is sent to your reader, the driver's phone will prompt them to approve the share. They have to tap 'approve.' This is automatic — you do not need to do anything extra.

Bottom Line

If your reader cannot verify it, it is not a valid mDL. Fall back to the physical license.

For a full explanation of what an mDL is and how the technology works, see DOC-01: Standards Overview.

How to Verify an mDL at a Traffic Stop

BEFORE YOU APPROACH

1. Open your mDL reader app on your assigned device.
2. Confirm it shows as ready — app open, no error messages.

AT THE VEHICLE

3. Request identification as you normally would.
4. If the driver says they have an mDL, tell them to open their wallet app and display the QR code on screen — OR hold their phone near your reader for NFC.
5. Scan the QR code with your reader, or initiate the NFC tap. Do not touch the driver's phone.
6. The driver's phone will prompt them to approve. Wait for them to tap approve.
7. Your reader displays the verified data — name, date of birth, address, DL number, license class and status, expiration date, and the driver's photo.
8. Compare the photo on your reader to the person in front of you, exactly as you would with a physical license.
9. Check the license status shown on your reader: valid, suspended, expired, or restricted.

AFTER THE VERIFICATION

10. If your reader is integrated with your CAD or reporting system, confirm that the mDL data has auto-populated your query fields, citation, or report. Correct any fields that did not populate.
11. Run your standard CIC/NCIC queries using the DL number captured from the mDL — same as any stop.
12. Complete the stop: issue citation, warning, or take other appropriate action.

Always Run Your Queries

Reading an mDL confirms the credential is authentic. It does not replace your database checks. Always run CIC/NCIC and any other required queries per agency policy.

For full workflow detail including downstream report integration (e-citation, crash report, arrest report, tow log), see DOC-04: Operational Workflows.

How to Use mDL Data in Your Reports

When your reader is integrated with your agency's CAD or field reporting software, mDL data works for you — it fills in the forms so you do not have to.

Report or Action	How mDL Data Helps
Electronic Citation (e-Citation)	Name, address, DOB, DL number, and license class auto-fill — no manual entry.
CIC / NCIC Query	DL number is auto-submitted, eliminating the transcription errors that cause missed hits.
Crash / Accident Report	All involved-party identity fields auto-populate. License status confirmed at point of contact.
Arrest Report	Booking identity comes from a verified credential — reduces identity errors at intake.
Vehicle Tow Log	Driver identity captured accurately at the time of tow.
Field Interview / Contact Card	Person contact record auto-populated and linked to your RMS master name index.

Data integration depends on the reader and CAD/FBR system your agency has deployed. If fields are not auto-populating, contact your agency's technology point of contact. See DOC-04: Operational Workflows for integration detail.

What to Do When Something Goes Wrong

Technology fails. Know what to do so the stop keeps moving.

If ...	Do This
The driver's phone is dead or damaged	Request the physical license. If they cannot produce one, follow your agency's standard procedures and applicable state law — which may include issuing a citation for failure to display a license upon demand.
Your reader cannot connect or establish a session	Request the physical license. If the driver cannot produce one, follow your agency's standard procedures and applicable state law. Report the reader failure to your agency's technology contact after the stop.
The driver declines to approve the share on their phone	Request the physical license. If they refuse to produce any ID, follow your standard protocol for an unidentified driver.
Your reader shows an authentication warning or failure	Do not accept the credential as valid. Treat the situation the same as if no credential was presented. Document the failure.
The mDL is from another state	Process it the same as an out-of-state physical license. If your reader is ISO/IEC 18013-5 compliant and has been loaded with that jurisdiction's public keys, it will authenticate the mDL. If it cannot, request the physical credential.
The driver shows a phone screen with a license image your reader cannot read	This is not a valid mDL. Request the physical credential. A visual display that cannot be read by your reader is not verified.
The driver claims to have an mDL but it is not working	Request the physical credential. If they have none, follow standard no-ID procedure.

For legal guidance on what officers can and cannot require during an mDL encounter, see DOC-07: Legal & Privacy Considerations.

What You Can and Cannot Do

YOU CAN

- Verify an mDL wirelessly without handling the driver's phone.
- Request only the data you need for the specific stop — name, DOB, DL number, license status, and photo for a routine traffic stop.
- Fall back to the physical credential at any point if the mDL cannot be verified.
- Require the physical credential — in most states, drivers are still legally required to carry one.

YOU CANNOT

- Look at or access any content on the driver's phone beyond the mDL session itself.
- Substitute a non-ISO digital product (photo, screenshot, or visual display) for a verified mDL — request the physical credential instead.
- Treat an unverified or flagged credential as valid.
- Assume everyone in the vehicle has an mDL — the holder must actively present it.

State laws on mDL acceptance vary. Know your jurisdiction's requirements and your agency's policy. See DOC-07: Legal & Privacy Considerations for full legal and privacy guidance.

Quick Reference — Traffic Stop at a Glance

1	Open reader app and confirm it is ready before approach.
2	Ask driver to open their wallet app and show the QR code — or hold phone near your reader for NFC.
3	Scan the QR code or tap NFC. Do NOT touch the driver's phone.
4	Wait for driver to approve the share on their phone.
5	Check the photo on your reader against the driver.
6	Check license status: valid, suspended, expired, or restricted.
7	Confirm mDL data auto-populated your citation / report / query fields.
8	Run CIC/NCIC queries per agency policy.
9	Complete the stop.
*	At any point — if the reader fails or the driver cannot present — request the physical license.

Related Toolkit Documents

- **DOC-01:** Standards Overview — what an mDL is, how it works, and the national deployment landscape
- **DOC-04:** Operational Workflows — full step-by-step workflow and downstream report integration detail
- **DOC-07:** Legal & Privacy Considerations — officer authority, data handling, and CJIS requirements
- **DOC-08:** Training Plan Framework — agency training curriculum and competency standards
- **DOC-10:** mDL FAQs for Law Enforcement — answers to common questions about mDL technology

LAW ENFORCEMENT mDL TOOLKIT
DOC-10

mDL FAQs for Law Enforcement
Mobile Driver License Frequently Asked Questions

Audience	All Law Enforcement Personnel
Purpose	Plain-language answers to the most frequently asked questions about ISO/IEC 18013-5 compliant Mobile Driver Licenses. Based on AAMVA mDL FAQ v2.6. All answers address ISO-compliant solutions only.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

Introduction

This document answers the questions officers most commonly ask about mobile driver licenses. Answers are intentionally brief. For deeper guidance on any topic, follow the references at the end of each answer or consult the related toolkit documents listed at the end of this guide.

All answers address ISO/IEC 18013-5 compliant mDL solutions. Non-ISO compliant digital products are addressed in Q11.

WHAT IS AN MDL

Q: What is an mDL?

A: A driver license or ID card issued by the state DMV and stored on a mobile device. It contains the same data as a physical license and can only be verified by an mDL reader.

For more detail, see DOC-01: Standards Overview.

Q: What is NOT an mDL?

A: A photo of a license, a screenshot, a digital image, or a picture of the barcode on the back of a license. None of these can be verified by a reader and none are valid mDLs.

See DOC-09: mDL Officer How-To Guide, Section 1.

EQUIPMENT AND VERIFICATION

Q: What does an officer need to read an mDL?

A: An mDL reader app or device issued by their agency — one capable of authenticating and displaying mDL data. A smartphone without an approved reader app installed is not sufficient.

See DOC-02: Hardware & Software Requirements and DOC-03: Available Devices & Software.

Q: Does the officer need to touch the driver's phone?

A: No. The officer never touches the driver's phone. All data transfers wirelessly from the driver's device to the officer's reader.

See DOC-09: mDL Officer How-To Guide for step-by-step instructions.

Q: Will the officer see a list of mDLs from people nearby in the reader app?

A: No. The officer's reader cannot detect whether anyone nearby has an mDL. The driver must actively open their wallet app and present it.

Q: How does the officer confirm the mDL belongs to the person in front of them?

A: The driver's photo is transmitted with the credential. The officer compares it to the person — the same as with a physical license.

Q: How does the officer know the mDL is real?

A: The reader automatically checks the DMV's digital signature. If it passes, the data is verified. If it fails, the reader shows a warning — do not accept that credential.

See DOC-04: *Operational Workflows* for guidance on authentication failures.

CONNECTIVITY AND INTEROPERABILITY

Q: Does the officer need cell service or internet to verify an mDL?

A: No. mDL verification is fully offline — device to device. Internet is still needed for CIC/NCIC queries and submitting reports.

See DOC-02: *Hardware & Software Requirements*.

Q: Can the officer read mDLs from other states?

A: If the reader is ISO/IEC 18013-5 compliant and has been loaded with the issuing jurisdiction's public keys, it will authenticate the mDL. Not all jurisdictions are in every reader's trust store — if the reader cannot verify the credential, request the physical license.

See DOC-01: *Standards Overview* for the current list of participating states.

WHEN THINGS DON'T WORK

Q: What if the driver cannot share their mDL, or the officer has no reader?

A: Request the physical credential and follow agency procedures and applicable state law. Depending on jurisdiction, failure to produce a valid license may be a citable offense.

See DOC-09: *mDL Officer How-To Guide*, Section 4 for a full failure-scenario reference table.

Q: What if the driver presents a non-ISO compliant digital product — a phone screen showing a license image?

A: Request the physical credential and follow standard procedures. A visual display that cannot be read by an ISO-compliant reader is not a valid mDL.

See DOC-01: *Standards Overview* for an explanation of ISO compliance.

Quick Reference

Question	Short Answer
What is an mDL?	A real DMV-issued license on a phone — same data as physical, digitally signed.
Is a photo of a license an mDL?	No. Photos, screenshots, and barcode images cannot be verified.
What equipment is needed?	An agency-issued mDL reader app or device with Bluetooth, NFC, and QR scanning.
Touch the driver's phone?	Never. All data transfers wirelessly.
Can I detect nearby mDLs?	No. The driver must actively present it.
How do I confirm it's the right person?	Compare the photo on your reader to the driver.
How do I know it's real?	Your reader checks the DMV's digital signature automatically.
Need internet or cell signal?	No — verification is offline. Internet is needed for queries and reports.
Out-of-state mDLs?	Readable if the reader has that jurisdiction's public keys loaded. If not, request the physical license.
Driver can't share / no reader?	Request physical credential. Follow standard no-ID procedures.
Non-ISO digital product?	Request physical credential. Visual-only displays are not valid mDLs.

Related Toolkit Documents

- **DOC-00:** Portfolio Overview — master index of all toolkit documents
- **DOC-01:** Standards Overview — how mDL technology works and the national deployment landscape
- **DOC-02:** Hardware & Software Requirements — device and software specifications
- **DOC-03:** Available Devices & Software — current market landscape
- **DOC-04:** Operational Workflows — full step-by-step procedures and report integration
- **DOC-07:** Legal & Privacy Considerations — officer authority, data handling, CJIS
- **DOC-08:** Training Plan Framework — agency training curriculum
- **DOC-09:** mDL Officer How-To Guide — step-by-step instructional field guide

Based on AAMVA mDL Frequently Asked Questions for Law Enforcement, Version 2.6. For the most current AAMVA guidance, visit aamva.org/topics/mobile-driver-license.