CNA



# ARTIFICIAL INTELLIGENCE IN LAW ENFORCEMENT: A PRIMER FOR LEADERS AND DECISION-MAKERS

Artificial intelligence (AI) is reshaping the public safety landscape, affecting how law enforcement agencies (LEAs) conduct investigations, analyze evidence, and utilize resources. Although these developments bring opportunities to enhance safety and efficiency, they also introduce new risks to evidentiary integrity, agency credibility, analytic rigor, civil liberties, and community trust. To mitigate these risks, command staff need a working understanding of what AI is, the applications of AI in law enforcement operations, the benefits and risks of specific AI use cases, and how to responsibly govern AI in ways that support constitutional, community-oriented policing. This primer discusses each of these areas and introduces a framework that law enforcement leaders can use to guide AI implementation in their agencies.

## What Is AI?

AI is an umbrella term that broadly refers to computer systems designed to perform tasks that typically require human intelligence, such as recognizing patterns, understanding language, making predictions, or generating content. AI systems can perform these tasks using such methods as the following:

- **Natural language processing (NLP):** Understands and generates human language.
- **Computer vision:** Interprets images and videos.
- **Generative AI:** Creates new content, such as text, images, audio, or code, in response to user inputs.
- **Predictive analytics:** Forecasts future outcomes using historical data.
- **Speech processing:** Understands spoken language and generates speech.
- **Machine learning:** Learns patterns from data to make predictions or decisions.

Many modern AI technologies combine several of these capabilities. For example, **large language models (LLMs)** are machine learning models trained on large amounts of text and other data to process and generate language. LLMs can support natural language processing and generative AI applications, and they underlie widely used applications such as ChatGPT, Gemini, and Claude. Similarly, an autonomous vehicle integrates computer vision, predictive analytics, and machine learning to perceive its surroundings and make driving decisions.

Most modern AI systems rely on machine learning to identify patterns in data and apply what they have learned to new information to support prediction, analysis, content generation, and decision-making. For law enforcement, these capabilities can enhance efficiency by assisting with tasks such as analyzing evidence, identifying public safety trends, summarizing information, and making informed decisions.

## AI Applications in Law Enforcement

Understanding AI capabilities is the first step toward identifying how they can add value in law enforcement. AI can support a broad range of administrative and operational functions, from analyzing information and drafting reports to identifying patterns and assisting with decision-making. Unlike many technologies traditionally used by police, AI is often embedded within existing software and workflows rather than deployed as a standalone application. For this reason, law enforcement executives should understand not only what AI is but also how it can be applied across agency operations. Table 1 illustrates how AI capabilities can be applied to common law enforcement functions and provides practical examples.

**Table 1. How AI can be applied to common law enforcement functions**

| Law Enforcement Function | AI Capability | How AI Is Applied | Illustrative Application |
|---|---|---|---|
| Investigations and digital evidence | NLP, speech processing, computer vision, machine learning, generative AI | Processes, organizes, and analyzes large volumes of investigative information and digital evidence | Transcription, translation, image or video analysis, link analysis, evidence triage, and identification of potentially relevant information or investigative leads |
| Identification and biometrics | Computer vision, speech processing, machine learning | Compares biometric characteristics against known or reference data to assist with identification | Facial recognition, fingerprint and voice matching, identity verification, and biometric comparisons |
| Surveillance and situational awareness | Computer vision, machine learning | Continuously analyzes video and sensor data to identify objects, events, or patterns that require attention | Automated alerts, anomaly detection, object recognition, sensor integration, and real-time monitoring |
| Analysis and resource planning | Machine learning, predictive analytics | Identifies patterns and forecasts trends to inform resource allocation and operational decisions | Pattern detection, demand forecasting, call triage, deployment support, and decision-support dashboards |
| Reporting and administration | NLP, generative AI, speech processing | Generates, summarizes, organizes, and processes information to reduce routine administrative work | Report drafting, records summarization, body-worn camera footage transcription and analysis, scheduling, and workflow support |

Source: CNA.

## Benefits and Risks for Law Enforcement

When carefully designed, tested, and governed, AI can provide a range of benefits that support core law enforcement goals, including increased efficiency, enhanced analytic capacity, and improved access to information. At the same time, AI systems can introduce or amplify risks related to data quality, system design, human decision-making, and oversight. Therefore, the benefits and risks of AI depend on how, where, and under what safeguards it is deployed. Figure 1 summarizes these benefits and risks in the context of law enforcement applications.

**BENEFITS**

- Reducing time spent on repetitive administrative tasks
- Helping personnel manage large volumes of digital evidence
- Surfacing patterns or connections that warrant human review
- Improving timeliness, accessibility, and organization of information
- Supporting more focused deployment of limited resources
- Enabling more sophisticated analysis of complex or unstructured information

**RISKS**

- Producing inaccurate, unsupported, or biased outputs
- Expanding surveillance capabilities or creating new civil-liberties concerns
- Complicating disclosure, evidentiary reliability, or auditability
- Exposing sensitive data through vendor systems or unclear data practices
- Eroding trust when use is hidden, poorly explained, or insufficiently supervised
- Encouraging overreliance on AI outputs or automation bias

Source: CNA.



## What Law Enforcement Leaders Should Ask and Act On

Understanding the potential benefits and risks of AI is only the first step. For law enforcement leaders, AI is a strategic leadership issue, not simply a technical one. The starting point should not be what AI can do but what the agency needs to accomplish.

Responsible adoption requires evaluating the operational value of an AI use case alongside its potential effects on rights, evidence, agency credibility, and public trust—and being prepared to limit, pause, or reject use cases that do not meet those standards. The five questions in Table 2 provide a practical framework for moving from identifying potential AI applications to making informed, accountable decisions about whether and how to deploy them. Rather than being addressed after deployment, these questions should be built into the entire implementation process, including procurement, policy development, pilot projects, and ongoing review.

**Table 2. Questions and Actions for Law Enforcement Leaders**

| Question | Leadership Action |
|---|---|
| **Purpose and use:** What problem are we solving, and is AI necessary and proportionate to the problem compared with other options? | **Clarify AI uses:** Intended purpose, alternatives, operational value, affected populations, potential effects on rights and public trust |
| **Governance and accountability:** Who is accountable for the system? Who can approve, supervise, audit, pause, or retire it? And what documentation is required? | **Lead governance:** Command accountability, decision authority, and clear roles for legal review, records, and community engagement |
| **Data and performance:** What data does the system use, how was it developed and tested, and how will we validate its accuracy and limitations in our own context? | **Evaluate data and systems:** Data quality, accuracy, bias, reliability, validation, evidentiary implications, and system limitations |
| **Implementation and safeguards:** Do our policies, contracts, training, and technical safeguards support responsible use? | **Align policy, procurement, and training:** Vendor and contracting, policies, supervision, audit trails, human decision authority, and role-specific training |
| **Oversight and trust:** How will we know whether the system continues to perform appropriately and maintain public trust? | **Reassess and report:** Rights and trust, complaints, disparate effects, legal developments, performance monitoring, reporting, reassessment, suspension, and retirement |

Source: CNA.

## Agency Readiness Is Critical

Answering these questions requires more than evaluating individual AI tools. Agencies also need to assess whether they have the organizational capabilities, governance processes, resources, and safeguards necessary to adopt and use AI responsibly. Rather than approaching AI adoption on an ad hoc, tool-by-tool basis, law enforcement agencies should consider their broader organizational readiness and identify capabilities that need to be developed or strengthened. CNA's AI Maturity Model for Government Agencies provides a framework for law enforcement leaders to do so, enabling agencies to assess their current level of AI maturity, establish desired future-state capabilities, identify gaps, and develop a roadmap for improvement. It addresses the breadth of activities needed for AI programs to be well governed and sufficiently resourced, as well as effective, trustworthy, safe, and secure.

CNA's Command Leadership for Emerging AI Readiness (CLEAR) Training complements this organizational approach by providing chiefs, sheriffs, command staff, and other agency leaders with practical knowledge and tools for making informed, defensible decisions about AI. Through an executive-focused curriculum addressing AI in policing, agency readiness, stakeholder communication, and agency-vendor relationships, CLEAR helps leaders translate AI concepts into decisions about governance, procurement, policy, training, oversight, and public trust.

Together, these approaches reinforce a central principle of responsible AI adoption: readiness does not depend on whether an agency has access to AI technology but rather on whether it has the leadership, governance, policies, people, and processes needed to use that technology effectively and responsibly.

## About CNA

The CNA Corporation (CNA) is a not-for-profit analytical organization dedicated to the safety and security of the nation. With nearly 700 scientists, analysts, and professional staff across the world, CNA's mission is to provide data-driven, innovative solutions to our nation's toughest problems. It operates the Center for Naval Analyses—the Department of the Navy's federally funded research and development center (FFRDC)—as well as the Institute for Public Research. The Center for Naval Analyses provides objective analytics to inform decision-making by military leaders and ultimately improve the lethality and effectiveness of the joint force. The Institute for Public Research leverages data analytics and innovative methods to support federal, state, and local government officials as they work to advance national and homeland security.

To learn more about AI in law enforcement at CNA, contact Cait Kanewske at kanewskel@ cna.org.

CNA® is a registered trademark of The CNA Corporation and may not be used without prior written authorization.



© 2026 The CNA Corporation