CNA

JULY 2026

Navigating the Artificial Intelligence Governance Landscape

Turning Regulatory Lessons into Readiness Strategies for Law Enforcement Agencies

Tammy Felix, Cait Kanewske, and Vivian Elliott
with contributions by Kaitlin DePartee

IIM-2026-U-044371-Final

CNA

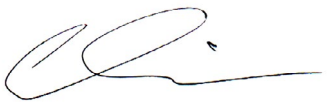
Abstract

As artificial intelligence (AI) rapidly reshapes policing, it introduces significant legal, ethical, and operational challenges. With federal AI regulations remaining largely voluntary, states are filling the void, creating a complex and fragmented regulatory landscape. This report provides law enforcement leaders with an early roadmap to navigate these emerging mandates. By analyzing landmark AI legislation from four early-adopter states, this paper identifies critical regulatory trends. California's legislation focuses on evidentiary integrity in police reporting, Texas's legislation focuses on transparency and prohibits some uses, Colorado's legislation focuses on high-risk algorithmic discrimination, and Utah's legislation focuses on disclosure-first public interactions. The analysis yields actionable insights for shaping procurement, data privacy, and human-oversight protocols. The report concludes by introducing a comprehensive AI Readiness Checklist. By applying these state-level lessons, law enforcement executives can transition from reactive compliance to proactive readiness, responsibly integrating AI while safeguarding constitutional rights, evidentiary reliability, and community trust.

This work was internally funded by CNA.

Cover image: Shutterstock.

Approved by: **July 2026**



David Kaufman, Vice President and Director
Safety and Security Division
CNA, Institute of Public Research

Executive Summary

Artificial intelligence (AI) is rapidly reshaping policing, from digital evidence management to officer wellness programs. But this increased efficiency comes with significant operational, administrative, and ethical challenges, specifically regarding transparency, civil rights, and public trust. In response, states are increasingly enacting legislation to regulate how AI is procured, deployed, and monitored.

This paper examines AI policies in California, Texas, Colorado, and Utah, states that were early adopters of governance requirements that directly affect law enforcement. Each state has taken a different approach:

- **California** has taken a targeted operational approach to AI-assisted police reporting, requiring disclosure, officer attestation, draft retention, audit trails, and limits on how vendors use law enforcement data.
- **Texas** has emphasized transparency and due process, requiring public disclosure of AI systems, notice to individuals affected by automated decisions, and avenues for human review and appeal.
- **Colorado** has taken the most restrictive approach, designating high-risk and prohibited uses, requiring annual impact assessments, and establishing explicit boundaries (i.e., redline policies) for systems such as predictive policing and facial recognition.
- **Utah** has focused on procurement oversight and risk management, mandating data minimization and enhanced vendor accountability before agencies can acquire AI systems.

Together, these state laws provide an early road map for how law enforcement agencies nationwide may be expected to manage AI. They also highlight the range of approaches emerging across jurisdictions, and they underscore the importance of preparing now for a complex and evolving regulatory landscape.

Key takeaways for law enforcement leaders

California Senate Bill 524 (Penal Code Section 13663)

California Senate Bill 524 regulates use of AI by law enforcement agencies in the following ways:

- **Transparency and disclosure.** Any police report generated fully or partially with AI must disclose (1) the AI program used and (2) whether the report was written fully or in part using AI.
- **Human review and accountability.** The officer or agency member who prepares the report must review and sign it, verifying that the facts are true and correct. This requirement preserves officer responsibility and makes clear that AI does not replace professional judgment.

- **Record retention and audit trails.** Agencies must retain the initial AI-generated draft of a report and maintain an audit trail identifying who used AI and what footage or audio informed the report. These requirements strengthen discovery, supervision, and evidentiary integrity.
- **Vendor controls.** Contracted vendors are restricted from sharing, selling, or otherwise using law enforcement data except for agency purposes or pursuant to court order, giving agencies a stronger basis for procurement and data-governance terms.

Texas Responsible AI Governance Act

The Texas Responsible AI Governance Act (TRAIGA) regulates AI use more broadly than does the California law, which is specific to law enforcement. TRAIGA applies to entities conducting business in the state and businesses whose products or services are used by Texas residents, among others. The act includes the following details relevant to law enforcement:

- **Prohibited uses.** The law prohibits certain AI applications that are relevant for law enforcement. For instance, it bans government entities from using AI for social scoring or for uniquely identifying individuals with biometric data without consent, with limited exceptions. This rule sets a clear precedent against using AI for broad social surveillance or unchecked biometric identification.
- **Data and privacy.** The law restricts law enforcement agencies from sharing sensitive information, such as personally identifiable information or biometric data, with unsecured third-party AI systems. All AI tools used must comply with strict data protection standards, and departments may not route sensitive case data to external, non-secure servers.
- **Transparency and oversight.** TRAIGA mandates that government agencies, including law enforcement, must provide clear, plain-language notice to the public when they are interacting with an AI system rather than a human. This rule requires departments to audit and train staff on how to disclose the use of AI properly.
- **Balancing innovation and risk.** Although TRAIGA imposes guardrails, it also includes a regulatory sandbox. This balance demonstrates recognition that regulation needs to leave room for innovation and testing. Other law enforcement agencies can learn from this model, which was designed with the understanding that responsible AI adoption may need to involve both explicit prohibitions and a structured environment for safely exploring new technologies.

Colorado Artificial Intelligence Act

The Colorado Artificial Intelligence Act establishes a comprehensive framework aimed at preventing algorithmic discrimination and ensuring accountability in automated decision-making. Key provisions that directly affect agency operations, compliance, and public trust include the following:

- **Definition of high-risk AI.** Systems that make or substantially influence decisions about jobs, housing, credit, health care, or legal outcomes are considered high risk. Law enforcement use of automated decision aids, such as predictive analysis facial recognition, may fall into this category.

- **Due process.** The law emphasizes that due process is central, mandating that individuals affected by AI-related decisions have access to notice, explanations, and a path for appeal.
- **Procurement of AI software.** The law requires vendors to provide technical documentation to support agency compliance. Law enforcement agencies must establish AI oversight structures, adopt standardized risk management processes, and ensure public disclosure of their use of AI.
- **Transparency and appeals.** Agencies must disclose when they use AI in decision-making and offer appeal mechanisms with human oversight (i.e., agencies must demonstrate a "human in the loop"); such disclosures are critical for maintaining procedural justice and public trust.

Utah Artificial Intelligence Policy Act

Taking a targeted approach to regulation, the Utah Artificial Intelligence Policy Act prioritizes clear disclosure and the mitigation of specific digital threats while still encouraging technological innovation. Important takeaways for public sector and law enforcement leaders include the following:

- **Transparency first.** Utah law mandates a "Transparency First" policy for agencies that requires them to have clear protocols to disclose when a citizen is interacting with an AI system, which is a crucial step for building public trust.
- **Definition of high-risk AI.** The law establishes a specific regulatory regime for high-risk applications, such as AI-driven wellness chatbots for officers, which signals that any program handling sensitive employee data will likely be a focal point for future regulations.
- **Prohibited uses.** Law enforcement leaders should take note of the law's focus on addressing the threats of deepfakes and manipulated content, which can be used to impersonate officers, spread misinformation, and undermine investigations.
- **Data and privacy.** To comply with this kind of legislation, law enforcement leaders should proactively inventory all generative AI uses within their departments, from administrative tools to public communication systems. They must also develop and implement clear disclosure protocols and strict policies to prevent the sale or misuse of data collected by these systems.
- **Balancing innovation and risk.** The Utah model demonstrates that a targeted "go slow, be smart" approach to AI governance can be an effective way to leverage new technologies while safeguarding both the public and law enforcement officers.

Navigating AI Governance Checklist

To help law enforcement leaders anticipate and manage these changes, The CNA Corporation (CNA) has developed an AI readiness checklist for police leaders.[1] This resource provides a practical, step-by-step guide for agencies to do the following:

[1] CNA's Command Leadership for Effective AI Readiness (CLEAR) Self-Assessment Tool is forthcoming.

- Establish governance and leadership structures (e.g., appoint an AI compliance lead, form oversight committees).
- Implement procurement and vendor controls, including requirements for audits and risk disclosures.
- Conduct pre-deployment and ongoing AI impact assessments.
- Build transparency measures, public engagement practices, and appeals processes.
- Define redline uses (e.g., social scoring, predictive policing, unregulated facial recognition, AI deepfakes) and ensure robust human oversight of consequential decisions.
- Safeguard data privacy, officer wellness applications, and community trust.
- Monitor emerging state and federal laws while preparing for future funding tied to governance policies.

By understanding the early regulatory actions of California, Texas, Utah, and Colorado and adopting tools such as CNA's AI Readiness Checklist, law enforcement leaders can move beyond reactive compliance toward proactive readiness. This preparation will enable departments to responsibly leverage the benefits of AI while upholding constitutional rights, maintaining legitimacy, and ensuring long-term sustainability in a rapidly evolving technological and legal environment.

Contents

Navigating the Governance Landscape

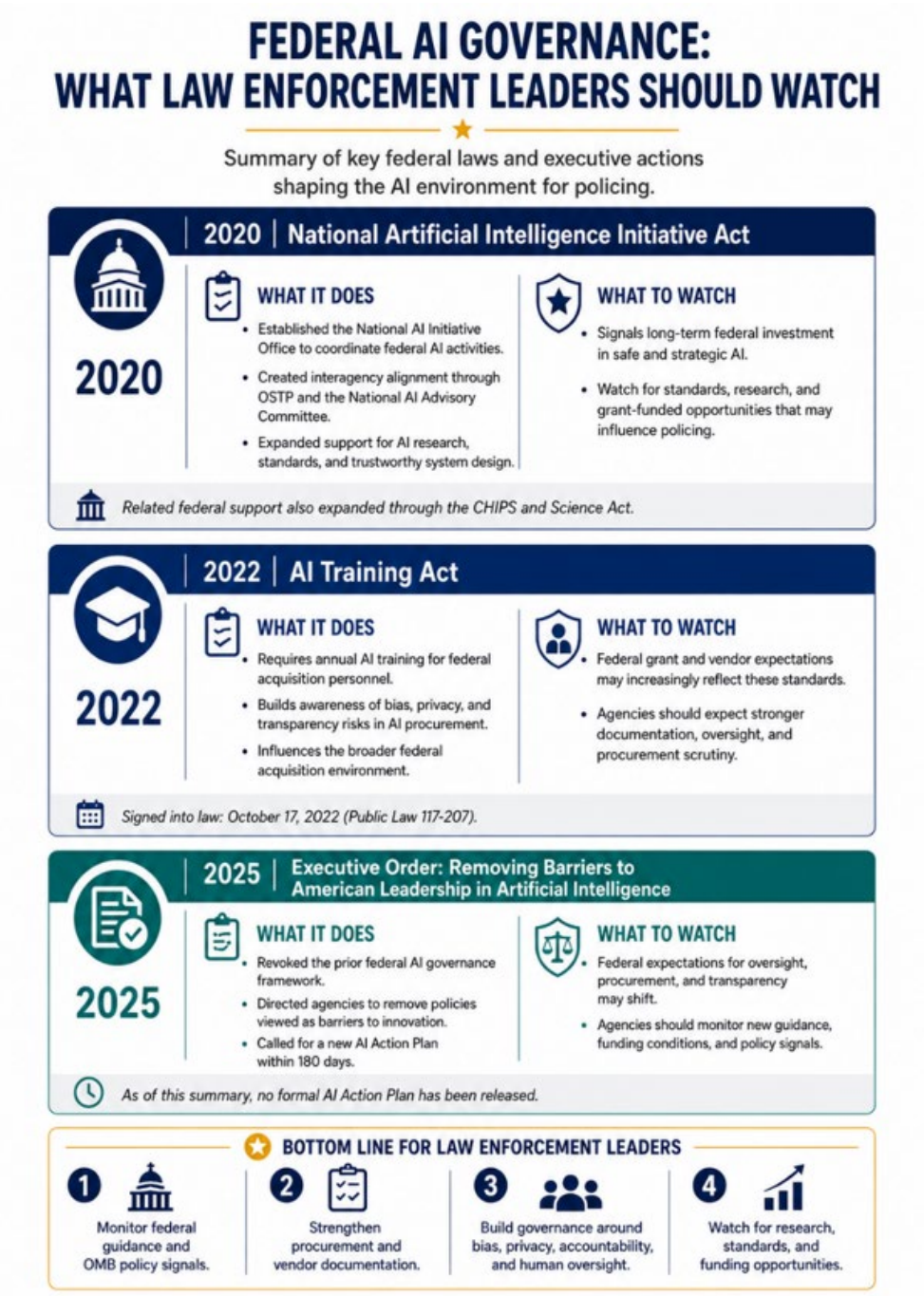
Federal frameworks and guidance

Federal laws and regulations around artificial intelligence (AI) are still evolving, and law enforcement leaders need to stay informed and aligned with emerging guidance. Hundreds of bills including the term *artificial intelligence* have been introduced since the 115th Congress (which met from January 2017 to January 2019), yet fewer than 30 laws have been enacted as of May 2025.[2] Federal frameworks are shaping expectations around transparency, human oversight, and responsible use of AI. Many of the proposed bills in the 118th and 119th Congresses have emphasized the development of voluntary guidelines, best practices, and industry-conducted evaluations of AI systems rather than prohibitions or independent evaluation of AI uses and technologies. Awareness of these standards helps agencies future-proof their policies, anticipate funding and compliance requirements, and build public trust in AI-enabled operations.

Figure 1 provides a snapshot of the federal regulations and guidance that departments should consider when developing strategies and policies to govern the responsible use of AI in policing.

[2] Laurie Harris, *Regulating Artificial Intelligence: U.S. and International Approaches and Considerations for Congress*, Congressional Research Service, R48555, 2025, https://www.congress.gov/crs-product/R48555.

Figure 1. Federal regulations and guidance on responsible AI integration



Source: CNA.

Although the federal government's approach appears to be more focused on overseeing federal government uses of AI than its use in the private sector, states are beginning to regulate AI to ensure fairness, transparency, and accountability.

Bridging the gap: Using state AI laws to inform law enforcement practice

This document provides case studies of four state-level AI laws in California, Texas, Colorado, and Utah that represent some of the earliest and most comprehensive efforts in the United States to regulate the use of AI.

Each case study summarizes (1) the scope and intent of the law, including requirements, prohibitions, and implications for law enforcement use of AI and (2) key takeaways for law enforcement leaders.

Law enforcement leaders can use this resource to do the following:

- **Anticipate regulatory trends.** Understand what types of AI uses (e.g., facial recognition, risk assessment tools, chatbots) policy-makers are targeting.
- **Assess agency readiness.** Benchmark an agency's current AI systems against emerging requirements, such as risk assessments, public disclosures, and human review safeguards.
- **Guide procurement and policy.** Use the lessons from California, Colorado, Texas, and Utah to shape vendor requirements, contracts, and internal governance before their state adopts similar rules.
- **Inform community engagement.** Prepare to explain to the public, oversight bodies, or city councils how their agency is addressing fairness, privacy, and transparency in AI use.

By reviewing these case studies, agencies can move beyond reactive compliance and start building proactive AI governance frameworks, which will position departments to maintain community trust, secure federal or state funding tied to responsible AI use, and avoid legal or reputational risks as regulation expands.

California: Senate Bill 524 (Penal Code Section 13663)

In 2025, California enacted Senate Bill (S.B.) 524, codified at Penal Code Section 13663 and effective January 1, 2026, to govern law enforcement use of AI in official police report writing. The law requires agencies to adopt a policy for AI-assisted reports and establishes clear requirements for disclosure, officer verification, draft retention, audit trails, and vendor data-use restrictions.

Key requirements and effects

California's approach is notable because it focuses directly on report integrity, evidentiary reliability, and accountability in law enforcement documentation rather than AI governance in the abstract. Figure 2 outlines considerations for the field in anticipation of, or in response to, similar regulations.

Figure 2. California S.B. 524: What does it cover and what can we learn?

Source: CNA.

Key takeaways for law enforcement leaders

California's law is important because it moves beyond general AI principles and addresses a specific operational use case already reaching the field: AI-assisted police report generation. Rather than banning this technology, the state requires agencies to use it in a way that preserves transparency, human review, auditability, and control over law enforcement data.

For law enforcement leaders, the practical implication is clear: agencies considering AI-enabled report-writing tools should not focus only on speed or reducing the administrative burden. They should also ensure that policies, training, records retention practices, supervisory review, and vendor agreements are strong enough to protect the integrity of official reports and withstand legal scrutiny.

Texas: Texas Responsible AI Governance Act

Texas enacted HB 149, the Texas Responsible AI Governance Act (TRAIGA), on June 22, 2025, effective January 1, 2026. It emphasizes prohibited uses (e.g., manipulation, unlawful deepfakes) and government transparency, establishes a seven-member government-appointed AI Council, and creates a regulatory sandbox allowing entities to test AI systems under relaxed regulations for up to 36 months.

Key requirements and effects

TRAIGA applies to developers and deployers of AI systems that do business in Texas or whose AI products and services are used by Texas residents. Under TRAIGA, the term *AI system* is defined broadly as any machine-based system that "use data to train statistical models for the purpose of enabling computer systems to perform tasks normally associated with human intelligence or perception, such as computer vision, speech or natural language processing, and content generation."[3] The definition is not limited to generative AI. Figure 3 outlines considerations for the field in anticipation of, or response to, similar regulations.

[3] Texas Responsible Artificial Intelligence Governance Act, H.B. 149, 89th Leg, 2025. https://legiscan.com/TX/text/HB149/id/3180120

Figure 3. TRAIGA: What does it cover and what can we learn?

Source: CNA.

Although some AI-related laws focus on specific sectors or applications, the Texas AI law stands out as one of the most comprehensive state-level regulations in the United States. It focuses on topics such as ensuring transparency, prohibiting certain uses, and providing government oversight. The law also recognizes the need to balance regulation with innovation, as evidenced by its creation of an advisory council and a regulatory "sandbox program" for testing new technologies in a controlled setting.[4] Any entity performing AI-related work in Texas or serving its residents should pay close attention to this statewide law.

TRAIGA appears to have been scaled back from earlier drafts. Many of the obligations and restrictions are narrower, and some broader requirements (e.g., requiring the private sector to mitigate foreseeable harms and complete extensive impact assessments) were removed or limited.[5] Prohibitions on practices such as biometric identification and social scoring primarily apply to governmental entities, and private-sector obligations in these areas are less stringent. By centralizing enforcement within the Texas Attorney General's Office, the law limits direct consumer recourse. This structure leaves definitions of several critical concepts (e.g., *manipulation*, *influence*, and *disclosure*) to be clarified through future legislation or legal interpretation.

Key takeaways for law enforcement leaders

Law enforcement agencies in other states should take note of TRAIGA because it represents the growing trend of state-level AI legislation. As a comprehensive framework, TRAIGA provides valuable insights into how these emerging laws can affect law enforcement operations. TRAIGA focuses on several key areas that are directly relevant to law enforcement use of AI:

- **Prohibited uses.** The law prohibits certain AI applications that are relevant for law enforcement. For instance, it bans governmental entities from using AI for social scoring or for uniquely identifying individuals with biometric data without consent, with limited exceptions. This detail sets a clear precedent against using AI for broad social surveillance or unchecked biometric identification.
- **Data and privacy.** The law restricts law enforcement agencies from sharing sensitive information, such as personally identifiable information or biometric data, with unsecured third-party AI systems. All AI tools used must comply with strict data protection standards, and departments may not route sensitive case data to external, nonsecure servers.
- **Transparency and oversight.** TRAIGA mandates that government agencies, including law enforcement, must provide clear, plain-language notice to the public when they are interacting with an AI system rather than a human. This requirement promotes a new level of transparency and requires departments to audit and train staff on how to properly disclose the use of AI.

[4] Maria Cruz Melendez, Stuart D. Levi, William E. Ridgway, and Brittany E. Libson, "Texas Charts New Path on AI with Landmark Regulation," Skadden, Arps, Slate, Meagher & Flom, June 23, 2025, https://www.skadden.com/insights/publications/2025/06/texas-charts-new-path-on-ai-with-landmark-regulation.
[5] "Texas Signs Responsible AI Governance Act into Law," Latham & Watkins, June 23, 2025, https://www.lw.com/en/insights/texas-signs-responsible-ai-governance-act-into-law.

- **Balancing innovation and risk.** Although TRAIGA imposes guardrails, it also includes a regulatory sandbox program. This inclusion demonstrates recognition that regulations need to leave room for innovation and testing. Other law enforcement agencies can learn from this model, understanding that responsible AI adoption involves both clear prohibitions and a structured environment for safely exploring new technologies.

TRAIGA serves as a significant model for law enforcement agencies nationwide, offering a glimpse into the future of AI regulation in policing. By addressing crucial issues such as prohibited uses, data privacy, and transparency, TRAIGA provides a clear framework for responsible AI adoption. Other states can learn from its approach of balancing innovation with risk through a regulatory sandbox, demonstrating that effective governance is not about halting progress but about establishing safe and ethical parameters. TRAIGA signals that law enforcement agencies must be proactive in developing policies that align with new legislative standards, ensuring that their use of AI is both effective for public safety and compliant with evolving legal and ethical norms.

Colorado: Colorado Artificial Intelligence Act

In 2024, the state of Colorado passed the Colorado Artificial Intelligence Act (CAIA) to prevent algorithmic discrimination. The law imposes specific responsibilities on developers and deployers of high-risk AI systems, which are defined as those that make "consequential" decisions affecting individuals' lives, such as those related to housing, employment, or health care. CAIA requires deployers to maintain a risk management program, conduct impact assessments before and annually after deployment, and notify individuals when an AI system is a substantial factor in an adverse decision.[6] Affected individuals must also be provided with the reasons for the decision and have access to an appeal process that includes human review. Developers, in turn, must provide documentation to deployers and notify the attorney general and customers of credible discrimination issues. The Colorado attorney general handles enforcement under state consumer protection law. Figure 4 outlines key considerations for the field in anticipation of, or response to, similar regulations.

[6] Mark W. Brennan, Katy J. Milner, J. Ryan Thompson, Sophie Baum, and Ambia Harper, "Colorado Becomes First U.S. State to Enact Broadly Applicable AI Law," Hogan Lovells, May 29, 2024, https://www.hoganlovells.com/en/publications/colorado-becomes-first-us-state-to-enact-broadly-applicable-ai-law.

Figure 4. The Colorado AI Act: What does it cover and what can we learn?

Source: CNA.

Key requirements and effects

Under CAIA, developers of AI systems are required to exercise "reasonable care" to prevent their algorithms from causing discriminatory outcomes.[7] They must also provide comprehensive documentation to the entities that deploy their AI systems. If developers become aware of a credible issue of discrimination related to their AI, they must notify both the Colorado attorney general and their customers within 90 days.

Meanwhile, deployers (the companies or organizations that use the AI systems) are mandated to establish and maintain a robust risk management program. They must also conduct impact assessments for these high-risk systems before their initial deployment, annually after deployment, and after any significant changes are made to the system.[8] Deployers are also responsible for providing individuals with notices, clear explanations for any adverse decisions made by the AI, and, where appropriate, a mechanism for appeals or human review.[9]

Enforcement of the law falls under the jurisdiction of the Colorado attorney general, who can act on violations using existing consumer protection laws.[10] Notably, developers and deployers who consistently adhere to the statute's requirements are granted a rebuttable presumption of "reasonable care," which can provide a legal defense in potential lawsuits.

This law is a landmark piece of legislation in the United States, and its approach to regulating AI is often compared to the European Union's AI Act. Both laws emphasize the importance of documented life-cycle governance and due process protections for individuals affected by high-stakes AI decisions, setting a precedent for how governments can proactively address the societal risks posed by AI technology.

Key takeaways for law enforcement leaders

The CAIA focuses on several core areas with direct implications for law enforcement applications of AI:

- **Definition of *high-risk AI*.** Systems that make or substantially influence decisions about jobs, housing, credit, health care, or legal outcomes are considered high risk. Many law enforcement tools, such as predictive analysis facial recognition and automated decision aids, may fall into this category.
- **Due process.** The law emphasizes that due process is central, mandating that individuals affected by AI-related decisions must have access to notice, explanations, and a path for appeal.
- **Procurement of AI software.** Vendors are required to provide technical documentation to help agencies comply with the law. To get ahead of these requirements, law enforcement leaders should establish an AI oversight committee, adopt standardized risk management templates, and prepare to publicly disclose their agency's use of AI.

[7] *Consumer Protections for Artificial Intelligence*, Colorado Senate Bill 24-205, § 6-1-1605(1).
[8] *Consumer Protections for Artificial Intelligence*, Colorado Senate Bill 24-205, § 6-1-1606(1).
[9] *Consumer Protections for Artificial Intelligence*, Colorado Senate Bill 24-205, § 6-1-1606(3).
[10] *Consumer Protections for Artificial Intelligence*, Colorado Senate Bill 24-205, § 6-1-1607.

- **Transparency and appeals.** Agencies must disclose when AI is used in decisions and offer an appeal mechanism with human oversight. Such disclosures are critical for maintaining procedural justice and public trust.

Utah: Artificial Intelligence Policy Act and 2025 updates

Utah's Artificial Intelligence Policy Act (AIPA) provides a legal framework that combines the following legislation:

- S.B. 149 AIPA (2024)
- S.B. 226 and SB 332 (amendments narrowing and refining AIPA and extending its duration)
- H.B. 452 (specific to AI "mental health chatbots" with added obligations)
- S.B. 271 (expands "abuse of personal identity" law to include AI-generated content in advertisement, fundraising, and endorsements)

Utah's model focuses on disclosure-first transparency and issue-specific protections rather than broad risk-tiering.

Key requirements and effects

In 2024, the Utah AIPA Amendments set new transparency and liability rules regarding generative AI, with a particular focus on consumer interactions. These amendments establish clear disclosure requirements for regulated occupations.[11] The law requires developers and deployers to inform users when they are interacting with a generative AI system in certain contexts. This obligation becomes stricter for regulated professions and instances when AI handles sensitive data or provides personalized advice related to legal, medical, or financial matters.

For mental health chatbots, the law creates a distinct set of regulations. These AI systems are subject to limitations on advertising and are prohibited from selling or sharing user health data.[12] They must also provide repeated disclosures to users and maintain clear policy documentation. In addition, the legislation broadens liability protections for individuals by expanding the legal recourse against the misuse of a person's identity, such as a scenario in which an AI-generated likeness is used without consent in endorsements, fundraising, or advertisements.

The Utah AI Amendments are notable because they establish some of the first consumer-facing transparency norms for generative AI in the United States. Unlike broader, tiered regulatory frameworks such as the European Union AI Act, Utah's approach provides a more targeted, issue-specific model that other states could adopt. The regulations specific to mental health chatbots are a pioneering example of how a state can regulate a particular high-risk application of AI without creating a comprehensive,

[11] Artificial Intelligence Amendments, S.B. 149, 2024 Gen. Sess. (Utah 2024). https://le.utah.gov/~2024/bills/static/SB0149.html
[12] Artificial Intelligence Amendments, H.B. 452, 2025 Gen. Sess. (Utah 2025). https://le.utah.gov/~2025/bills/static/HB0452.html

economy-wide system. Figure 5 outlines key considerations for the field in anticipation of, or in response to, similar regulations.

Figure 5. Utah's AI governance laws: What do they cover and what can we learn?

Source: CNA.

Key takeaways for law enforcement leaders

The state of Utah has provided a clear roadmap for law enforcement leaders and other government agencies on how to adopt AI technology responsibly. Its approach prioritizes transparency and specific, actionable safeguards rather than broad, sweeping regulations. This model can serve as a guide for other agencies looking to get ahead of the evolving legal landscape around AI.

AIPA focuses on several key areas that are directly relevant to law enforcement use of AI:

- **Prioritizing transparency.** The Utah law mandates a "Transparency First" policy for agencies that requires them to have clear protocols for disclosing when a citizen is interacting with an AI system, which is a crucial step in building public trust.
- **Managing high-risk applications.** The law establishes a specific regulatory regime for high-risk applications, such as AI-driven wellness chatbots for officers. This approach signals that any program handling sensitive employee data will likely be a focal point for future regulations.
- **Preventing misinformation.** Law enforcement leaders should also take note of the law's focus on addressing the threats of deepfakes and manipulated content, which can be used to impersonate officers, spread misinformation, and undermine investigations.
- **Auditing AI inventories.** To comply with this kind of legislation, law enforcement leaders should proactively inventory all generative AI uses within their departments, from administrative tools to public communication systems. They must also develop and implement clear disclosure protocols and strict policies to prevent the sale or misuse of data collected by these systems.
- **Adopting incremental governance.** The Utah model demonstrates that a targeted, "go slow, be smart" approach to AI governance can be an effective way to leverage new technologies while safeguarding both the public and law enforcement officers.

Ensuring proactive readiness

The evolving landscape of AI governance, exemplified by the legislation in California, Texas, Colorado, and Utah, offers a clear set of lessons for law enforcement leaders. The first and most critical takeaway is the need for proactive readiness. Rather than waiting for mandates, law enforcement agencies should immediately inventory all current and potential uses of generative AI. With a current inventory complete, departments can preemptively develop clear disclosure protocols and safeguards, which are essential for building and maintaining public trust. As Utah's approach demonstrates, transparency is paramount, and citizens must be informed when an AI system is involved in public-facing interactions.

Law enforcement leaders must also recognize that regulatory frameworks will likely be targeted toward specific high-risk applications. The strict safeguards placed on AI-driven wellness chatbots and high-risk uses of AI in consequential decision-making are prime examples, signaling that applications handling sensitive data will be heavily scrutinized. Departments must also actively address the growing threat of AI-generated misinformation, such as deepfakes, by establishing policies that protect the identities and

reputations of both officers and the public. By adopting these principles of transparency, targeted governance, and proactive planning, law enforcement agencies can responsibly integrate AI, ensuring operational effectiveness and public confidence in the digital age.

Learning from California, Texas, Colorado, and Utah

California, Texas, Colorado, and Utah offer distinct models for AI governance. California takes a targeted operational approach to AI-assisted police reporting, requiring disclosure, officer attestation, draft retention, audit trails, and limits on vendor use of law enforcement data. Colorado emphasizes algorithmic fairness in high-risk decisions with strict obligations for developers and deployers. Utah focuses on disclosure and safeguards for sensitive interactions, especially in regulated professions and mental health chatbots. Texas takes a broader approach, banning manipulative uses, mandating government transparency, and launching an AI Council and regulatory sandbox program. Although enforcement mechanisms vary across the four states, each state's approach reflects a growing expectation that agencies and vendors maintain thorough documentation, provide clear consumer notice, and ensure meaningful oversight. Figure 6 provides a detailed side-by-side comparison.

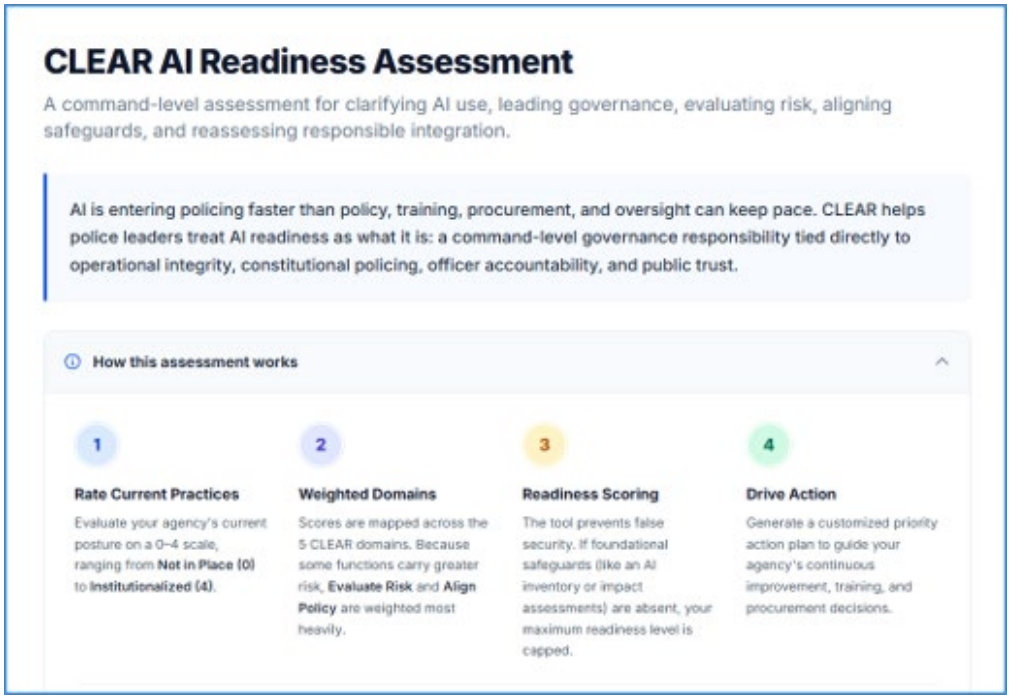
Figure 6. Comparing AI governance in California, Texas, Colorado, and Utah

Source: CNA.

CNA's AI Readiness Resource

CNA's forthcoming *Command Leadership for Emerging Artificial Intelligence Readiness (CLEAR) AI Readiness Assessment* tool is designed to help law enforcement leaders benchmark their agency's AI systems against emerging standards for transparency, risk management, and human oversight. Drawing from federal guidance, state legislation, and the National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF), it offers a practical tool for assessing readiness and shaping policies. Figure 7 provides an overview of the four-step evaluation process used in CNA's *CLEAR AI Readiness Assessment* tool.

Figure 7. CNA's CLEAR AI Readiness Assessment



Source: CNA.

As departments work to anticipate the potential effects of AI on law enforcement operations, observing lessons learned from other jurisdictions and peer agencies may be useful. CNA's checklist provides a foundation for building a comprehensive AI governance framework for law enforcement agencies. It is a proactive guide designed to highlight the key considerations for governing the responsible use of AI tools in policing, investigations, and justice operations. It draws on the NIST AI RMF, state-level legislation (S.B. 524, TRAIGA, CAIA, and AIPA), and federal guidance from the US Department of Justice, Department of Homeland Security, and Office of Management and Budget. Agencies can use this checklist to assess their

readiness and guide policy development by clicking the checkboxes to track progress as they complete each step.

Figures

Additional Reading

"AI Inventory." US Department of Justice. Updated Jan. 30, 2026. https://www.justice.gov/ai/ai-inventory.

AI Training Act. S.2551, Public Law 117-207. https://www.congress.gov/bill/117th-congress/senate-bill/2551.

Artificial Intelligence Amendments. Utah S.B. 149. 2024. https://le.utah.gov/~2024/bills/static/SB0149.html.

Artificial Intelligence Amendments. Utah S.B. 452. 2025. https://le.utah.gov/~2025/bills/static/HB0452.html.

Baker Botts. "DOJ Releases AI-related Compliance Guidance." Sept. 2024. https://www.bakerbotts.com/thought-leadership/publications/2024/september/doj-releases-ai-related-compliance-guidance.

Carr, Ashley, Sean Fulton, Karley Buckley, Kyle Kloeppel, and Kathryn Cote. "Texas Adopts the Responsible AI Governance Act (TRAIGA)." DLA Piper. June 26, 2025. https://www.dlapiper.com/en/insights/publications/2025/06/texas-adopts-the-responsible-ai-governance-act.

Concerning Consumer Protections in Interactions with Artificial Intelligence Systems (Revised). Colorado S.B. 24-205. 2024. https://leg.colorado.gov/sites/default/files/documents/2024A/bills/2024a_205_rer.pdf.

Concerning Consumer Protections in Interactions with Artificial Intelligence Systems (Signed). Colorado S.B. 24-205. 2024. https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf.

Consumer Protections for Artificial Intelligence (Enrolled Bill Text). Colorado S.B. 24-205. 2024. https://leg.colorado.gov/bills/sb24-205.

Gluck, Justine. *Overview of Utah's 2025 Enacted AI Legislation*. Future of Privacy Forum. Apr. 2025. https://fpf.org/wp-content/uploads/2025/04/Overview-of-Utahs-2025-Enacted-AI-Legislation.pdf.

Lords, Tiyanna Danielle. "Colorado Enacts Law Regulating High-risk Artificial Intelligence Systems." Business Law Today. July 23, 2024. https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-july/colorado-enacts-law-regulating-high-risk-artificial-intelligence-systems/.

Mayorkas, Alejandro N. Policy Statement 139-06 for Department of Homeland Security Agency and Office Leaders. Subject: Acquisition and Use of AI Technologies. Aug. 8, 2023. https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_139-06-acquistion-use-ai-technologies-dhs-components.pdf.

National Institute of Standards and Technology. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. 2023. https://www.nist.gov/itl/ai-risk-management-framework.

Silverboard, Dan M., Jennifer Rangel, and Maddie McNamara. "Texas Enacts Comprehensive AI Governance Laws with Sector-specific Healthcare Provisions." Holland & Knight. June 27, 2025. https://www.hklaw.com/en/insights/publications/2025/06/texas-enacts-comprehensive-ai-governance-laws.

Texas Senate Research Center. Bill Analysis (Texas Responsible Artificial Intelligence Governance Act, C.S.H.B. 149). May 20, 2025. https://capitol.texas.gov/tlodocs/89R/analysis/html/HB00149S.htm.

US Department of Justice. *Compliance Plan for OMB Memorandum M-24-10*. Mar. 27, 2024. https://www.justice.gov/media/1373026/dl.

US Department of Justice Office of Legal Policy. *Artificial Intelligence and Criminal Justice: Final Report*. Dec. 3, 2024. https://www.justice.gov/olp/media/1381796/dl.

References

Artificial Intelligence Amendments, S.B. 149, 2024 Gen. Sess. 2024. https://le.utah.gov/~2024/bills/static/SB0149.html.

Artificial Intelligence Amendments, H.B. 452, 2025 Gen. Sess. 2025. https://le.utah.gov/~2025/bills/static/HB0452.html.

Brennan, Mark W., Katy J. Milner, J. Ryan Thompson, Sophie Baum, and Ambia Harper. "Colorado Becomes First U.S. State to Enact Broadly Applicable AI Law." Hogan Lovells. May 29, 2024. https://www.hoganlovells.com/en/publications/colorado-becomes-first-us-state-to-enact-broadly-applicable-ai-law.

Consumer Protections for Artificial Intelligence, S.B. 24-205, 74th Gen. Assemb., Reg. Sess. 2024. https://leg.colorado.gov/bills/sb24-205.

Cruz Melendez, Maria, Stuart D. Levi, William E. Ridgway, and Brittany E. Libson. "Texas Charts New Path on AI with Landmark Regulation." Skadden, Arps, Slate, Meagher & Flom. June 23, 2025. https://www.skadden.com/insights/publications/2025/06/texas-charts-new-path-on-ai-with-landmark-regulation.

Harris, Laurie. *Regulating Artificial Intelligence: U.S. and International Approaches and Considerations for Congress*. Congressional Research Service. R48555. 2025. https://www.congress.gov/crs-product/R48555.

"Texas Signs Responsible AI Governance Act into Law." Latham & Watkins. June 23, 2025. https://www.lw.com/en/insights/texas-signs-responsible-ai-governance-act-into-law.

Texas Responsible Artificial Intelligence Governance Act, H.B. 149, 89th Leg., Reg. Sess. 2025. https://legiscan.com/TX/text/HB149/id/3180120.

This report was written by CNA's Safety and Security Division (SAS).

SAS works to help improve decision-making during crisis operations and foster innovative solutions to challenges in the areas of public safety, emergency management, public health preparedness, homeland security, risk management, and national security.

Dedicated to the Safety and Security of the Nation

www.cna.org

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.

IIM-2026-U-044371-Final