



Brief: HB 1170

Bill Summary

HB 1170, introduced in the 2026 Virginia General Assembly Session, requires the Department of Criminal Justice Services to develop a model policy for the use of covered artificial intelligence systems. Subsequently, each local law enforcement agency, sheriff's department, and the Department of State Police must establish and adopt a written AI policy and make it publicly available. HB 1170 was tabled in committee.

Policy Landscape

Currently, there are no states where legislation was the mechanism to require a state agency to require law enforcement to have a broader AI policy. Multiple states, including Virginia, do have existing laws that require state agencies to develop policies for specific AI-enabled technologies. For example, Utah¹ and California² have laws that require disclosures on AI-written police reports which are similar, but narrower, than Virginia's HB 1294³. Similarly, in Virginia, state law requires the State Police to establish a model policy governing law enforcement use of facial recognition technology (FRT).⁴ These measures focused on disclosures surrounding specific technologies rather than the requirement of a general AI policy, which was the intent of HB 1170.

Although no state has adopted a law identical to HB 1170, both the federal government and various state legislatures have increasingly taken broader approaches to AI governance that are consistent with HB 1170's approach. For example, in response to an executive order,⁵ the Office of Management and Budget issued [guidance](#) requiring US federal agencies to conduct annual inventories of **all** their AI use cases and make this information publicly available. This requirement applies to AI broadly, rather than to specific AI-enabled technologies.

Similarly, states have begun enacting comprehensive AI laws governing state entities using AI, multiple of which include a requirement for a state agency to establish an AI model policy. For example, Maryland requires the Department of Information Technology to adopt policies governing the use of high-risk AI systems by government entities.⁶ Connecticut similarly requires the Office of Policy and Management to establish policies governing the use of AI systems by state agencies.⁷

Outside of the US, the United Kingdom has created an *AI Action Plan for Justice*⁸. This plan both encourages the use of AI throughout the criminal justice system and establishes cross cutting principles to ensure its safe use. Additionally, the Ministry of Justice published an *AI and Data Science Ethics Framework*⁹ followed by its *Engineering AI Governance Framework*¹⁰, both specifically relating to criminal justice services. Lastly, the UK also has an Algorithmic

Transparency Standard, which requires government agencies to publish clear, accessible information about how and why they use algorithmic tools and AI in decision-making.

The European Union's AI Act takes a comprehensive approach to regulating AI and defines AI broadly.¹¹ For example, Article 5(1)(d) of the EU AI Act prohibits certain practices, including the use of AI risk assessments for predicting criminal activity as well as untargeted facial scraping to create or expand facial recognition databases¹².

Primary Stakeholders

- Department of Criminal Justice Services
- Virginia Sheriffs Association
- Virginia State Police
- Chiefs of Police Association
- Virginia Association of Commonwealth's Attorneys
- Indigent Defense Commission

Questions for Consideration

1. Is DCJS the best entity to oversee this requirement?

The Virginia Department of Criminal Justice Services (DCJS) is charged with planning and carrying out programs and initiatives to improve the functioning and effectiveness of the criminal justice system as a whole¹³. However, in the bill's fiscal impact statement¹⁴, DCJS indicated that they did not currently have the capacity to take on this additional responsibility. They estimated the cost to be an initial \$450,000 with \$200,000 ongoing to support a full-time position.

The overall intent of the bill is to ensure that Virginia law enforcement agencies that are using AI have a use policy to ensure adequate governance over this use. To ease any policy writing burden on individual agencies and to ensure consistency for this general-purpose technology, the bill vests authority in a state-level agency to develop a model policy to serve as a baseline that individual agencies can adopt or use as a guide. The authority to develop a model policy need not rest with DCJS; rather, it is appropriate for any state-level agency that has experience with law enforcement agencies. For example, the patron may consider collaborating with the Office of the Attorney General and/or the Virginia State Crime Commission to identify an alternative to DCJS. The State Police would be another viable option. In fact, Virginia's facial recognition technology (FRT) law similarly directs the State Police to develop a model policy governing FRT use.¹⁵ That existing framework could serve as a model for assigning responsibility under HB 1170.

Regardless of the collaboration that is sought, the need for both criminal justice and technical expertise is a significant issue. Therefore, the patron may also consider reaching out to the Virginia IT Agency (VITA) for guidance on establishing the necessary technical expertise.

2. Does "law enforcement officer" defined in Va. Code 9.1-101, capture the intended population?

Although the bill uses the term "law enforcement agency" rather than "law enforcement officer," Virginia law defines "law enforcement officer" broadly in Va. Code § 9.1-101.¹⁶ If the bill relies on that existing definition, it could unintentionally encompass a wide range of state agencies beyond traditional policing agencies, such as:

- Virginia Lottery
- Department of Motor Vehicles
- Virginia Marine Police
- Department of Wildlife Resources
- Department of Conservation and Recreation

It is possible that some of these agencies may use AI in different manners than "traditional" law enforcement agencies and should therefore be considered when obtaining stakeholder input.

To avoid ambiguity, consider defining law enforcement agencies specific to this bill and limit the scope to state and local police departments, sheriff's offices, and prosecutors. For example, Virginia's domestic violence statute defines law enforcement, in part, as employees of a "police department or sheriff's office which is part of or administered by the Commonwealth or any political subdivision thereof."¹⁷ This bill could take a similar approach, defining "law enforcement agencies" to include only state and local police departments and sheriff's offices that are part of or administered by the Commonwealth or any political subdivision thereof.

3. Should the bill require a specific framework?

There is a proliferation of available AI tools¹⁸ that purport to enable a multitude of tasks within criminal justice such as streamlining processing¹⁹ or identifying individuals²⁰. As these technologies become more prevalent, the need for clear guardrails is heightened. In response, lawmakers may want to consider how it approaches technologies specifically being used for consequential activities within the criminal justice system.

There is an argument for establishing guiding principles in legislation but allowing subject matter experts to enumerate a specific framework. This allows for the framework to evolve as the technology evolves and for the technical specifications to be flexible and consider industry best practices, while adhering to certain outcomes that are required by law (e.g. fairness, non-discrimination). If this approach is preferred, review and revision periods should be considered a requirement to ensure these benefits.

To the extent that a specific framework would be helpful, there are certain minimum requirements that a model policy could include. For example, the bill could ensure that there are rules governing data collection to prevent unnecessary or arbitrary collection of personal information; rules governing data retention to help reduce the risk of privacy intrusions; and basic transparency requirements. The Policing Project's AI Policy Guidance and IACP's Technology Policy Framework provide a useful framework for identifying these baseline safeguards.²¹

Additional Considerations

- Should the model policy exclude disclosure of AI used solely for internal training purposes?
- How should disclosure be handled in cases where the local law enforcement body does not have a public facing website?
- With AI becoming ubiquitous in software, how can it be defined to ensure the model policy is both meaningful and actionable, encompassing both stand-alone AI systems and AI embedded in other applications?
- How will the governing agency that develops the model policy, incentivize smaller localities to comply? How will the adoption of the model policy by localities be enforced?
- Considering the pace at which technologies are evolving, at what frequency should a model policy be re-visited?

Recent Relevant Publications

In addition to the citations throughout this brief, the following articles and frameworks may provide insight into both the problem and potential solutions.

- *Police AI Policy Guidance*²² - NYU Policing Project
- *Principles for the Use of AI in Criminal Justice*²³ - Council on Criminal Justice
- *An AI Taxonomy for Criminal Justice*²⁴ - RAND/Council on Criminal Justice
- *AI in Criminal Justice: Why Governance Matters and How to Make it Work*²⁵ – Stanford Law & Policy Lab

References

- ¹ "SB0180," accessed July 2, 2026, <https://le.utah.gov/%7E2025/bills/static/SB0180.html>.
- ² "SB 524- CHAPTERED," accessed July 2, 2026, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260SB524.
- ³ "HB1294 - 2026 Regular Session | LIS," accessed July 2, 2026, <https://lis.virginia.gov/bill-details/20261/HB1294>.
- ⁴ "SB 524- CHAPTERED."
- ⁵ "Removing Barriers to American Leadership in Artificial Intelligence," Federal Register, January 31, 2025, <https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence>.
- ⁶ "View Document - Maryland Code and Court Rules," accessed July 24, 2026, [https://govt.westlaw.com/mdc/Document/N3EC694A0351D11EF97F0A3407294726C?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=\(sc.Default\)](https://govt.westlaw.com/mdc/Document/N3EC694A0351D11EF97F0A3407294726C?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default)).
- ⁷ "Chapter 50 - Office of Policy and Management: General Provisions; Budget and Appropriations; State Planning," accessed July 24, 2026, https://cga.ct.gov/current/pub/chap_050.htm#sec_4-68jj.
- ⁸ "AI Action Plan for Justice," GOV.UK, accessed July 6, 2026, <https://www.gov.uk/government/publications/ai-action-plan-for-justice/ai-action-plan-for-justice>.
- ⁹ "Ministry of Justice AI and Data Science Ethics Framework," GOV.UK, accessed July 6, 2026, <https://www.gov.uk/government/publications/ministry-of-justice-ai-and-data-science-ethics-framework>.
- ¹⁰ "Engineering AI Governance Framework," MoJ Technical Guidance, accessed July 6, 2026, <https://technical-guidance.service.justice.gov.uk/documentation/governance/ai-governance-framework.html>.
- ¹¹ *Article 2: Scope | EU Artificial Intelligence Act*, n.d., accessed July 24, 2026, <https://artificialintelligenceact.eu/article/2/>.
- ¹² *Article 5: Prohibited AI Practices | EU Artificial Intelligence Act*, n.d., accessed July 6, 2026, <https://artificialintelligenceact.eu/article/5/>.
- ¹³ "§ 9.1-102. (Effective July 1, 2027) Powers and Duties of the Board and the Department," accessed July 6, 2026, <https://law.lis.virginia.gov/vacode/9.1-102/>.
- ¹⁴ "HB1170 - 2026 Regular Session | LIS," accessed July 6, 2026, <https://lis.virginia.gov/bill-details/20261/HB1170>.
- ¹⁵ "§ 52-4.5. (Effective until July 1, 2026) Facial Recognition Technology; Authorized Uses; Department to Establish a State Police Model Facial Recognition Technology Policy; Penalty," accessed July 24, 2026, <https://law.lis.virginia.gov/vacode/title52/chapter1/section52-4.5/>.
- ¹⁶ "§ 9.1-101. Definitions," accessed July 9, 2026, <https://law.lis.virginia.gov/vacode/9.1-101/>.
- ¹⁷ "§ 19.2-81.3. Arrest without a Warrant Authorized in Cases of Assault and Battery against a Family or Household Member and Stalking and for Violations of Protective Orders; Procedure, Etc," accessed July 24, 2026, <https://law.lis.virginia.gov/vacode/title19.2/chapter7/section19.2-81.3/>.
- ¹⁸ Eric Bloedorn et al., *IAN SPECIAL SERIES: AI-1 | ARTIFICIAL INTELLIGENCE APPLICATION APPROACHES FOR LAW ENFORCEMENT*, n.d.
- ¹⁹ "Existing AI Tools for Criminal Defense," *UC Berkeley Law*, n.d., accessed July 2, 2026, <https://www.law.berkeley.edu/research/criminal-law-and-justice-center/our-work/ai-for-public-defenders/existing-ai-tools/>.

²⁰ "A Forensic Without the Science," accessed July 2, 2026, <https://www.law.georgetown.edu/privacy-technology-center/research/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/>.

²¹ "AI Policies," The Policing Project, accessed July 24, 2026, <https://www.policingproject.org/ai-policies>.

²² The Policing Project, "AI Policies."

²³ "Principles for the Use of AI in Criminal Justice - Council on Criminal Justice," October 30, 2025, <https://counciloncj.org/principles-for-the-use-of-ai-in-criminal-justice/>.

²⁴ "An AI Taxonomy for Criminal Justice - Council on Criminal Justice," May 12, 2026, <https://counciloncj.org/an-ai-taxonomy-for-criminal-justice/>.

²⁵ Stanford Law School, "AI in Criminal Justice: Why Governance Matters and How to Make It Work," Stanford Law School, accessed July 24, 2026, <https://law.stanford.edu/publications/ai-in-criminal-justice-why-governance-matters-and-how-to-make-it-work/>.