

26102711D

1 **HOUSE BILL NO. 797**

2 Offered January 14, 2026

3 Prefiled January 13, 2026

4 A BILL to amend the Code of Virginia by adding a section numbered 2.2-2012.01 and by adding in Chapter  
5 20.1 of Title 2.2 an article numbered 9, consisting of sections numbered 2.2-2034.2 through 2.2-2034.7,  
6 relating to Virginia Information Technologies Agency; artificial intelligence; independent verification  
7 organizations.  
8

9 Patron—Hayes

10 Committee Referral Pending  
11

12 Be it enacted by the General Assembly of Virginia:

13 1. That the Code of Virginia is amended by adding a section numbered 2.2-2012.01 and by adding in  
14 Chapter 20.1 of Title 2.2 an article numbered 9, consisting of sections numbered 2.2-2034.2 through  
15 2.2-2034.7, as follows:16     *§ 2.2-2012.01. Additional duties of the CIO relating to licensing of independent verification  
17 organizations of artificial intelligence.*18     *The CIO shall have the power and duty to oversee the licensing of independent verification organizations  
19 (IVOs) of artificial intelligence pursuant to Article 9 (§ 2.2-2034.2 et seq.). The CIO shall promulgate  
20 regulations necessary or incidental to the licensing of such IVOs, which shall include:*21         *1. Conflict of interest and funding transparency requirements, including reporting requirements  
22 regarding the IVOs' funding sources and revenue generation and self-audit requirements regarding the IVOs'  
23 board composition to ensure adequate independence from the artificial intelligence industry;*24         *2. Requirements for identifying additional IVO plan elements as needed to ensure acceptable levels of risk  
25 from IVO-verified artificial intelligence systems or applications;*26         *3. Provisions on circumstances mandating corrective action or loss of license;*27         *4. Requirements related to the structure and terms of the Artificial Intelligence Safety Advisory Council,  
28 including the procedures for appointing additional members; and*29         *5. Requirements related to IVO application procedures and required materials.*

30             Article 9.

31             *Independent Verification Organizations of Artificial Intelligence.*32     *§ 2.2-2034.2. Definitions.*33     *As used in this article, unless the context requires a different meaning:*34     *"Artificial intelligence application" means a software program or system that uses artificial intelligence  
35 systems to perform tasks that typically require human intelligence.*36     *"Artificial intelligence system" means any machine learning-based system that, for any explicit or implicit  
37 objective, infers from the inputs such system receives how to generate outputs, including content, decisions,  
38 predictions, and recommendations, that can influence physical or virtual environments. "Artificial  
39 intelligence system" does not include any artificial intelligence system or general purpose artificial  
40 intelligence model that is used for development, prototyping, and research activities before such artificial  
41 intelligence system or general purpose artificial intelligence model is made available to deployers or  
42 consumers.*43     *"Deployer" means a person or entity that implements, integrates, or makes operational an artificial  
44 intelligence system or artificial intelligence application within the Commonwealth. "Deployer" includes a  
45 person or entity that makes an artificial intelligence system or artificial intelligence application available for  
46 use by others within the Commonwealth, whether directly or as part of a product or service.*47     *"Developer" means a person or entity that develops an artificial intelligence system or artificial  
48 intelligence application that is deployed in the Commonwealth.*49     *"Independent verification organization" or "IVO" means a person or entity licensed by the Virginia  
50 Information Technologies Agency (VITA) pursuant to this article to assess artificial intelligence systems' or  
51 applications' adherence to standards reflecting best practices for the prevention of personal injury and  
52 property damage.*53     *"Security vendor" means a third-party entity engaged by an IVO or developer to evaluate the safety or  
54 security of an artificial intelligence system or application, including by using processes such as red teaming,  
55 risk detection, and risk mitigation.*56     *§ 2.2-2034.3. Licensing of independent verification organizations.*57     *A. Each person or entity seeking to act as an IVO within the Commonwealth shall obtain a license from  
58 VITA.*

INTRODUCED

HB797

59       B. An application for an IVO license shall be made by filing with VITA the information, materials, and  
60 forms required by this article and the regulations promulgated by the CIO pursuant to § 2.2-2012.01, along  
61 with a plan detailing all of the following information:

62       1. The risks with respect to which the applicant intends to verify that artificial intelligence systems or  
63 artificial intelligence applications implement mitigation measures sufficient to achieve acceptable levels of  
64 risk. For each such risk, the applicant shall submit (i) a proposed definition of acceptable levels of risk; (ii)  
65 metrics that are measurable and can be used to determine whether the acceptable level of risk defined by the  
66 IVO produces beneficial outcomes; (iii) target levels for the metrics, including data sources such levels are  
67 based on and methods for measurement; and (iv) a description of the evaluation and reporting protocol to  
68 determine whether verified models or applications meet the outcome metrics on an ongoing basis.

69       2. Proposed technical, operational, governance, and other mitigation requirements for developers or  
70 deployers, including procedures for pre-development and post-development, to ensure acceptable levels of  
71 risk, including ongoing monitoring of risks and assessment of mitigation efficacy.

72       3. Methodologies and sources used to evaluate the efficacy of mitigation requirements and updates to  
73 such methodologies and sources as needed.

74       4. Benchmarks, technologies, and audit methodologies proposed to assess developer and deployer  
75 adherence to mitigation requirements.

76       5. Approach to assessing continued good standing of a developer or deployer, including reviewing and  
77 evaluating the developer's or deployer's maintenance of artificial intelligence governance plans and policies,  
78 processes for risk monitoring and mitigation, whistleblower protections, and training for employees and third  
79 parties.

80       6. Disclosure requirements for developers or deployers related to detected risks, incident reports, or  
81 material changes to risk profiles, including both risks detected prior to verification and risks resulting from  
82 fine-tuning or modifying an artificial intelligence system or artificial intelligence application after  
83 verification.

84       7. Procedures for prescribing and verifying implementation of corrective actions to remedy an identified  
85 failure by a developer or deployer to do any of the following: (i) achieve an acceptable level of risk with  
86 respect to an artificial intelligence application or artificial intelligence system; (ii) comply with any other  
87 mitigation requirements promulgated by the applicant; or (iii) comply with the developer's or deployer's  
88 artificial intelligence governance plans and policy.

89       8. Standards and procedures for revoking verification for noncompliance with the applicant's mitigation  
90 requirements, failure to achieve acceptable levels of risk, or noncompliance with the developer's or  
91 deployer's artificial intelligence governance plans and policies.

92       9. Whether the applicant proposes market-specific verification and how plans are tailored to that  
93 segment.

94       10. Coordination with federal and state authorities.

95       11. Personnel qualifications.

96       12. Governance policies, sources of funding, and policies ensuring independence.

97       13. Any other information required by VITA.

98       C. VITA may license an applicant as an IVO if (i) such applicant demonstrates independence from the  
99 artificial intelligence industry and (ii) every element of the applicant's submitted plan is adequate to ensure  
100 that artificial intelligence systems or artificial intelligence applications verified pursuant to such plan will  
101 mitigate to an acceptable level one or more risks including as defined by the metrics the applicant proposes.  
102 If verification is proposed by an applicant for a specific market segment, VITA shall evaluate the applicant's  
103 submitted plan accordingly. If VITA finds that an applicant's plan adequately mitigates some, but not all, of  
104 the proposed risks, the applicant shall be licensed to verify only those risks for which the plan is deemed  
105 adequate.

106       D. An IVO issued to an applicant by VITA shall specify the risks the IVO is authorized to verify and any  
107 market segments for which the license applies.

108       E. VITA shall establish reasonable application and renewal fees sufficient to offset administrative costs.  
109 Such fees shall be payable to VITA and used for (i) application processing, (ii) audits of IVOs, (iii)  
110 compensation of the Artificial Intelligence Safety Advisory Council, and (iv) general administration of this  
111 article.

#### 112       § 2.2-2034.4. License revocation.

113       A. VITA shall revoke an IVO license if it determines any of the following:

114       1. The IVO's plan is materially misleading or inaccurate;  
115       2. The IVO fails to adhere to its plan in a way that materially impairs its responsibilities, including failure  
116 to adhere to the plan's procedures for ongoing monitoring of verified artificial intelligence systems or  
117 applications and implementation of corrective action;

118       3. A material change compromises independence from the artificial intelligence industry;

119       4. Technological evolution renders methods obsolete for ensuring acceptable levels of the risk VITA has  
120 designated the independent verification organization to verify; or

121       5. A verified model or application causes material harm of the type the IVO defines an acceptable level of  
 122 risk in order to prevent.

123       B. If VITA determines the public interest so requires, it may allow an IVO to cure the basis for revocation  
 124 before terminating the license.

125       **§ 2.2-2034.5. Independent verification organization responsibilities; modifications to plans.**

126       A. A licensed IVO shall implement the approved plan submitted pursuant to subsection B of § 2.2-2034.3,  
 127 which includes verifying artificial intelligence systems or artificial intelligence applications. An IVO shall  
 128 revoke verification of an artificial intelligence system or artificial intelligence application if a developer or  
 129 deployer (i) fails to meet mitigation requirements, (ii) fails to cooperate with monitoring, (iii) violates  
 130 governance policies, or (iv) fails to implement corrective actions.

131       B. An IVO may (i) update or modify the following aspects of the approved plan: (a) technical and  
 132 operational requirements; (b) evaluation benchmarks; (c) audit methodologies; (d) governance plans; or (e)  
 133 any other element of its plan in order to take advantage of improved technology; (ii) address previously  
 134 discovered issues with its plan; or (iii) otherwise enhance the efficacy of its verification activities.

135       **§ 2.2-2034.6. Annual reporting.**

136       A. An IVO shall submit an annual report to VITA including:

137       1. Aggregated information on the capabilities of the artificial intelligence systems and artificial  
 138 intelligence applications evaluated by the IVO, the observed societal risks and benefits associated with those  
 139 capabilities, and the potential societal risks and benefits associated with those capabilities;

140       2. Adequacy of evaluation resources, technical capabilities, and mitigation measures to address observed  
 141 and potential risks;

142       3. Aggregated results of verification assessments;

143       4. Aggregated and anonymized compliance with prescribed remediation;

144       5. Anonymized descriptions of any additional, significant risk the IVO observed while conducting its  
 145 assessments, even if such risk is not one the IVO is licensed to verify;

146       6. A list of verified artificial intelligence systems;

147       7. A description of evaluation methods; and

148       8. Governance or funding changes affecting independence.

149       B. An IVO may redact trade secrets, sensitive business information, personally identifiable information,  
 150 and other security-sensitive content.

151       C. Documentation used in reports shall be retained for 10 years. An IVO shall also retain all  
 152 documentation relating to its assessment and verification of artificial intelligence systems or applications,  
 153 including ongoing monitoring and any subsequent corrective action, for 10 years following the relevant  
 154 activity.

155       D. VITA shall publish redacted versions of reports submitted by IVOs pursuant to this section online.

156       **§ 2.2-2045.7. Artificial Intelligence Safety Advisory Council.**

157       A. The Chief Information Officer shall establish and appoint members to the Artificial Intelligence Safety  
 158 Advisory Council (the Council) for the purpose of advising and assisting VITA in licensing and auditing  
 159 IVOs.

160       B. The membership of the Council shall not exceed 12 and shall include at least one citizen representative  
 161 from a nongovernmental organization, educational and research institution, public policy institute, or  
 162 consumer and business advocacy organization. All members of the Council shall be qualified to assess IVO  
 163 plans. Members shall serve four year terms and no member may serve more than two consecutive terms.  
 164 Members may be removed for inefficiency, neglect, or malfeasance. A majority of the members of the Council  
 165 shall constitute a quorum. Members shall serve without compensation but shall be reimbursed for all  
 166 reasonable and necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.

167       C. Members of the Council shall (i) refrain from any action or occupation, gainful or not, that is  
 168 incompatible with their duties, including employment by a developer or deployer of artificial intelligence; (ii)  
 169 refrain from owning or acquiring any equity or other interest, directly or indirectly, in companies whose  
 170 business consists in significant part of developing or deploying artificial intelligence; and (iii) observe a one-  
 171 year post-employment restriction from any artificial intelligence firms or IVOs.

172       D. The Council shall keep a record of its proceedings, including any considerations relating to the  
 173 issuance, refusal, renewal, or revocation of IVO licensure.