26106161D

HOUSE BILL NO. 1521

Offered January 23, 2026

A BILL to amend the Code of Virginia by adding in Title 59.1 a chapter numbered 58, consisting of sections numbered 59.1-607 through 59.1-616, relating to digital innovation and infrastructure; establishing rights in digital property and technology resources; requiring risk management policies for critical infrastructure facilities controlled by critical artificial intelligence systems; providing safe harbors; preempting local regulation; and providing for enforcement and remedies.

Patron—Williams

Referred to Committee on Communications, Technology and Innovation

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding in Title 59.1 a chapter numbered 58, consisting of sections numbered 59.1-607 through 59.1-616, as follows:

CHAPTER 58.

VIRGINIA DIGITAL INNOVATION AND INFRASTRUCTURE ACT.

§ 59.1-607. Legislative findings and intent.

A. The General Assembly finds that:

1. Innovations in technology, including machine learning and artificial intelligence, enable breakthroughs across every sector of the economy, driving economic growth, creating jobs, and improving quality of life for all Virginians;

2. The Commonwealth of Virginia is home to the largest concentration of data center infrastructure in the world and serves as the headquarters or site of major operations for globally significant technology companies, representing billions of dollars in capital investment and tens of thousands of jobs, and maintaining a regulatory environment that attracts and retains such investment is essential to the Commonwealth's continued economic prosperity;

3. Ensuring that the Commonwealth and the United States remain at the forefront of technology development is critical for driving economic growth, safeguarding national security, and retaining a competitive edge in the global economy;

4. While recognizing the benefits of innovations in technology, some applications of powerful systems may pose risks to public health and safety that warrant reasonable, targeted regulation;

5. Federal and state governments increasingly propose restrictions on the ability to privately own or make use of technology resources for lawful purposes, some of which may burden fundamental constitutional rights without adequate justification; and

6. A uniform statewide regulatory framework for technology resources and artificial intelligence systems is necessary to prevent a patchwork of local regulations that could deter investment, fragment markets, and impede innovation.

B. The General Assembly finds that the rights to acquire, possess, and protect property under Article I, Section 11 of the Constitution of Virginia, and the freedoms of speech and press under Article I, Section 12 of the Constitution of Virginia, encompass the right to own and make use of technology resources for lawful purposes. Any restriction placed by the Commonwealth, or any county, city, town, or other political subdivision thereof, on the ability to privately own or make use of technology resources for lawful purposes shall be subject to strict scrutiny and shall be valid only if it is narrowly tailored to serve a compelling government interest and is the least restrictive means of achieving that interest.

C. The General Assembly declares that nothing in this chapter shall be construed to diminish the rights of consumers under the Virginia Consumer Data Protection Act (§ 59.1-575 et seq.) or the rights of individuals with respect to digital assets under the Uniform Fiduciary Access to Digital Assets Act (§ 64.2-116 et seq.).

§ 59.1-608. Definitions.

As used in this chapter, unless the context requires a different meaning:

"Artificial intelligence system" means a machine-based system that, for explicit or implicit objectives, infers from inputs it receives how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments.

"Critical artificial intelligence system" means an artificial intelligence system that is designed and deployed to autonomously control, or to be a substantial factor in controlling, the operations of a critical infrastructure facility without contemporaneous human oversight. The term does not include:

1. An artificial intelligence system that performs a narrow procedural task, improves the result of a previously completed human activity, performs a preparatory task for an assessment relevant to a human decision, or detects decision-making patterns or deviations from preexisting decision-making patterns;

2. Antifraud, antimalware, antivirus, cybersecurity, database, data storage, firewall, networking, spam-filtering, spell-checking, spreadsheet, web-caching, web-hosting, or search engine technologies, or similar technologies that do not autonomously control physical infrastructure; or

3. A technology that communicates in natural language for the purpose of providing users with information, making referrals or recommendations, answering questions, or generating content, provided such technology is subject to an acceptable use policy that prohibits the generation of content that is unlawful under federal or state law.

"Critical infrastructure facility" means any of the following facilities that provide essential services to the public:

1. An electrical power generating facility, substation, switching station, or electrical control center;

2. A chemical, polymer, or rubber manufacturing facility;

3. A water intake structure, water treatment facility, wastewater treatment plant, or pump station;

4. A natural gas compressor station, processing plant, storage facility, or liquefied natural gas terminal;

5. A telecommunications central switching office or remote terminal;

6. A port, railroad switching yard, trucking terminal, or other freight transportation facility;

7. A transmission facility used by a federally licensed radio or television station;

10. A steel-making facility that uses an electric arc furnace;

11. A facility identified and regulated under the United States Department of Homeland Security Chemical Facility Anti-Terrorism Standards program;

12. A dam regulated by the Commonwealth or the federal government; or

13. Any portion of an aboveground oil, gas, hazardous liquid, or chemical pipeline.

"Deployer" means a person that deploys a critical artificial intelligence system to control, in whole or in part, a critical infrastructure facility. The term does not include a person that develops or licenses an artificial intelligence system to another person for deployment.

"Digital asset" means an electronic record in which a person has a right or interest. The term has the same meaning as in § 64.2-116. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic record.

"Government action" means any law, ordinance, regulation, rule, policy, permit, license, condition, or administrative practice enacted, adopted, or enforced by a government entity that restricts the common or intended use of technology resources or digital assets.

"Government entity" means the Commonwealth, or any county, city, town, or other political subdivision thereof, and any branch, department, division, agency, board, commission, authority, or instrumentality of the Commonwealth or of any such political subdivision.

"Risk management policy" means a written policy that identifies, assesses, and provides for the mitigation of reasonably foreseeable risks posed by a critical artificial intelligence system to the safe and reliable operation of a critical infrastructure facility.

"Technology resources" means tools, technologies, systems, or infrastructure, whether digital, analog, or otherwise, that facilitate data processing, storage, transmission, manipulation, control, creation, dissemination, or use of information or data. The term includes hardware, software, algorithms, sensors, networks, protocols, platforms, services, systems, cryptographic applications, machine learning systems, and quantum computing applications.

§ 59.1-609. Rights in digital property and technology resources.

A. A government action that restricts the ability of a person to privately own or make use of technology resources for lawful purposes shall be valid only if it is narrowly tailored to serve a compelling government interest and is the least restrictive means of achieving that interest.

B. Digital assets, including digital content, computer files, cryptocurrency, tokens, virtual property, and other data stored or recorded electronically, are personal property, and a person has the right to acquire, possess, use, protect, and transfer such property as provided by law.

C. The owner of technology resources or digital assets has the following rights:

1. The right to control access to such technology resources and digital assets;

2. The right to transfer ownership of such digital assets;

3. The right to delete or modify such digital assets, except as otherwise provided by law;

4. The right to possess and use technology resources for any lawful purpose; and

5. The right to be secure against unreasonable searches and seizures of such digital assets and technology resources.

D. No government entity shall compel disclosure of a private cryptographic key, password, or other credential used to secure digital assets or technology resources except pursuant to a warrant issued by a court upon a finding of probable cause, supported by oath or affirmation, particularly describing the place to be searched and the persons or things to be seized.

E. Seizure and forfeiture.

4. Nothing in this chapter shall limit the authority of law enforcement to seize digital assets or technology resources pursuant to a warrant issued upon probable cause, or pursuant to a judicially recognized

exception to the warrant requirement, in connection with the investigation or prosecution of a criminal offense.

5. No permanent forfeiture of digital assets or technology resources to the Commonwealth or any political subdivision thereof shall be ordered except upon a criminal conviction of the owner for an offense to which the assets are substantially connected, or as authorized by federal law.

§ 59.1-610. Risk management for critical infrastructure controlled by critical artificial intelligence systems.

A. A deployer that deploys a critical artificial intelligence system to control, in whole or in part, the operations of a critical infrastructure facility shall develop, maintain, and abide by a risk management policy.

B. A risk management policy shall be reasonable in light of the nature and scope of the critical infrastructure facility's operations and the role of the critical artificial intelligence system in those operations. In determining reasonableness, a deployer shall consider guidance and standards set forth in:

6. The most recent version of the Artificial Intelligence Risk Management Framework published by the National Institute of Standards and Technology;

7. ISO/IEC 42001 or any successor standard published by the International Organization for Standardization; or

8. Another nationally or internationally recognized risk management framework for artificial intelligence systems.

C. A deployer shall review and update its risk management policy at least annually, and more frequently if there is a material change in the critical artificial intelligence system or its use.

D. Compliance with a risk management plan prepared pursuant to federal law or regulation that addresses substantially the same risks as a risk management policy required by this section shall constitute compliance with subsections A through C.

§ 59.1-611. Safe harbor.

A. A deployer that develops, maintains, and abides by a risk management policy in compliance with § 59.1-610 shall not be liable under state law for damages arising from a failure of the critical artificial intelligence system if the deployer demonstrates that:

9. The deployer had in effect at the time of the alleged failure a risk management policy that complied with the requirements of § 59.1-610;

10. The deployer was in substantial compliance with the risk management policy at the time of the alleged failure; and

11. The alleged failure was not the result of willful misconduct or gross negligence by the deployer.

B. The safe harbor established by subsection A shall not apply to:

12. Claims for personal injury or wrongful death;

13. Claims arising from intentional or knowing violations of law by the deployer;

14. Claims arising under federal law; or

15. Actions brought by the Attorney General pursuant to § 59.1-614.

C. Nothing in this section shall be construed to create a private right of action against a deployer for failure to comply with § 59.1-610.

§ 59.1-612. Annual attestation.

A. On or before July 1 of each year, a deployer subject to § 59.1-610 shall file with the Secretary of Commerce and Trade an attestation, signed by an officer or authorized representative of the deployer, certifying that:

16. The deployer has developed and maintains a risk management policy in compliance with § 59.1-610; and

17. The deployer is in compliance with the risk management policy.

B. The attestation shall identify the critical infrastructure facility or facilities and the critical artificial intelligence system or systems to which it applies. The attestation shall not require disclosure of proprietary or confidential business information, trade secrets, or information the disclosure of which would create a security vulnerability.

C. The Secretary of Commerce and Trade shall maintain a registry of attestations filed pursuant to this section. The registry shall be a public record, except that any information identified by the deployer as confidential pursuant to subsection B shall not be disclosed.

D. A deployer that fails to file an attestation as required by this section shall not be entitled to assert the safe harbor provided by § 59.1-611.

§ 59.1-613. Uniform regulation; local preemption.

A. The regulation of technology resources, digital assets, and artificial intelligence systems is a matter of statewide concern requiring uniform regulation throughout the Commonwealth.

B. No county, city, town, or other political subdivision of the Commonwealth shall adopt or enforce any ordinance, resolution, regulation, or policy that:

18. Restricts the ownership, possession, or lawful use of technology resources or digital assets in a

manner inconsistent with this chapter;

19. Imposes requirements on deployers of artificial intelligence systems that are in addition to or inconsistent with the requirements of this chapter; or

20. Prohibits or requires prior governmental approval for the deployment of an artificial intelligence system for a lawful purpose, except as expressly authorized by state or federal law.

C. Any ordinance, resolution, regulation, or policy adopted by a political subdivision in violation of this section shall be void and unenforceable.

D. Nothing in this section shall be construed to preempt or limit the authority of a political subdivision to:

21. Regulate land use, zoning, noise, or other physical impacts of data centers or other technology infrastructure in accordance with otherwise applicable law;

22. Enforce building codes, fire codes, or other health and safety regulations of general applicability; or

23. Adopt policies governing its own use of artificial intelligence systems in the provision of government services.

§ 59.1-614. Enforcement and remedies.

A. Any person whose rights under this chapter have been violated by a government entity may bring an action in the circuit court of the county or city in which the violation occurred, or in which the person resides, to:

1. Obtain a declaratory judgment that a government action violates this chapter;

2. Obtain injunctive relief to prevent a government entity from enforcing a government action that violates this chapter;

3. Recover actual damages sustained as a result of the violation;

4. Recover reasonable attorney fees and costs if the person substantially prevails; and

5. obtain any other relief the court deems appropriate.

B. The Attorney General may bring an action to enforce this chapter against:

24. A government entity that has adopted or is enforcing a government action in violation of this chapter; or

25. A deployer that has failed to file an attestation as required by § 59.1-612 or that has filed a materially false attestation.

C. In an action brought by the Attorney General against a deployer pursuant to subdivision B 2, the court may impose a civil penalty not to exceed $10,000 for each violation, in addition to any other relief the court deems appropriate.

D. A court may declare that a government action is void and unenforceable if it determines that such action violates the provisions of this chapter.

§ 59.1-615. Construction; preservation of law enforcement authority.

A. Nothing in this chapter shall be construed to:

1. Authorize, legalize, or provide a defense to any conduct that constitutes a criminal offense under federal or state law;

2. Limit the authority of law enforcement to investigate, seize evidence of, or prosecute criminal offenses, including offenses involving the sexual exploitation of minors, controlled substances, fraud, money laundering, terrorism, or other crimes;

3. Prevent a court from issuing a warrant, subpoena, or other lawful process in connection with a criminal investigation or prosecution;

4. Create any right or immunity for a person who uses technology resources or digital assets to facilitate, commit, or conceal criminal activity; or

5. Limit any forfeiture authorized by federal law.

B. Nothing in this chapter shall be construed to alter, diminish, or interfere with the rights and remedies available under federal or state intellectual property laws, including patent, copyright, trademark, and trade secret laws.

C. Nothing in this chapter shall be construed to preempt, supersede, or limit the application of federal law.

§ 59.1-616. Effective date.

The provisions of this chapter shall become effective on July 1, 2026, except that § 59.1-612, requiring annual attestations, shall become effective on July 1, 2027.

2. That the provisions of this act shall become effective on July 1, 2026, except as otherwise provided in § 59.1-616 of this act.

2. That the provisions of this act shall become effective on July 1, 2026, except as otherwise provided in § 59.1-616 of this act.