

VEHICLE AUTONOMY AND SECURITY ACT OF 2026

A BILL

To protect the security, privacy, freedom of movement, and transportation autonomy of the American people by establishing uniform national requirements governing connected vehicles, vehicle telemetry, remote vehicle communications, remote access and control systems, and associated software and hardware in all motor vehicles manufactured, imported, sold, resold, or introduced into interstate commerce in the United States, without regard to the country of origin of the vehicle, manufacturer, software, hardware, service provider, or controlling entity.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Vehicle Autonomy and Security Act of 2026”.

SEC. 2. FINDINGS AND PURPOSE.

Congress makes the following findings:

- (1) Reliable access to independently operable motor vehicles is critical to the economic security, physical security, freedom of movement, emergency preparedness, and individual autonomy of the people of the United States.
- (2) Motor vehicles constitute essential transportation infrastructure and, in many areas of the United States, represent the principal or only practical means by which individuals may evacuate, obtain food, obtain medical care, travel to employment, assist family members, or otherwise respond to a natural disaster, cyberattack, communications outage, armed conflict, civil emergency, national emergency, or other adverse event.
- (3) Modern connected vehicles incorporate advanced information and communications technologies capable of collecting, processing, storing, and transmitting substantial quantities of information, including geolocation information, vehicle-operating information, driver behavior, diagnostic information, audio or visual information, and other personal or operational information.
- (4) Connected vehicles may also incorporate hardware and software capable of receiving remote commands, modifying vehicle functionality, restricting vehicle functionality, installing software, changing vehicle configuration, determining vehicle location, or otherwise affecting the operation of the vehicle without direct physical access to the vehicle.

(5) The risks created by such capabilities do not depend solely upon the nationality or country of origin of the manufacturer, developer, supplier, telecommunications provider, data processor, or governmental entity having access to such capabilities.

(6) Unauthorized or unnecessary access to vehicle connectivity systems by any foreign or domestic corporation, government agency, contractor, service provider, data broker, telecommunications provider, or other third party may create risks of surveillance, data exploitation, cyber intrusion, remote manipulation, disruption of transportation, and loss of individual autonomy.

(7) A vehicle manufactured by a corporation organized under the laws of the United States may present substantially similar risks to individual privacy, transportation security, and vehicle autonomy as a vehicle manufactured outside the United States if the vehicle incorporates systems capable of continuous telemetry, remote tracking, remote control, remote disablement, or unnecessary transmission of vehicle or occupant information.

(8) The security of the American people therefore requires a uniform standard based upon the capabilities and conduct of a vehicle and its associated systems rather than the geographic location in which the vehicle or component was manufactured.

(9) Americans should have access to motor vehicles that remain capable of their essential transportation functions independently of continuous external communications, manufacturer servers, cloud-computing infrastructure, subscription services, cellular networks, satellite networks, internet connectivity, or other remotely operated infrastructure.

(10) Except for narrowly defined functions necessary to satisfy an immediate safety requirement or a communication knowingly initiated or expressly authorized by the vehicle owner or operator, a motor vehicle should not require the continuous transmission of information concerning the vehicle, its occupants, its location, or its operation to a manufacturer, laboratory, data center, government agency, contractor, service provider, or other remote entity.

(11) No manufacturer, domestic corporation, foreign corporation, Federal agency, contractor, or other entity should possess unrestricted technical capability to remotely disable, immobilize, materially restrict, or assume control over a privately owned motor vehicle merely because such capability has become technologically feasible.

(12) A uniform national vehicle-autonomy standard will strengthen the resilience of the United States transportation system by ensuring that vehicles remain useful during communications failures, cyberattacks, infrastructure disruptions, natural disasters, national emergencies, and other adverse conditions.

SEC. 3. DEFINITIONS.

(1) CONNECTED VEHICLE.

The term “connected vehicle” means a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways that—

(A) integrates onboard networked hardware with automotive software systems to communicate through dedicated short-range communications, cellular telecommunications connectivity, satellite communication, Wi-Fi, Bluetooth, radio-frequency communications, or any other wireless communications technology with another network or device; or

(B) is designed, manufactured, or originally equipped to communicate by such means, regardless of whether that capability is enabled, disabled, dormant, subscription-dependent, or removed at the time of importation, manufacture, sale, resale, or introduction into interstate commerce.

(2) VEHICLE TELEMETRY.

The term “vehicle telemetry” means information generated, collected, stored, processed, or transmitted by or through a motor vehicle concerning—

(A) the geographic location or historical movement of the vehicle;

(B) speed, acceleration, braking, steering, throttle position, or other driver behavior;

(C) vehicle operation or usage;

(D) diagnostic or mechanical information;

(E) occupants or users of the vehicle;

(F) audio, video, biometric, or sensor information associated with an occupant;

(G) paired devices, communications, contacts, identifiers, or other personal information;

(H) charging, fueling, battery, or energy-consumption information; or

(I) any other information that can reasonably be associated with an identifiable vehicle, owner, operator, passenger, or device.

(3) REMOTE VEHICLE ACCESS.

The term “remote vehicle access” means the technological capability of a person or system not physically connected to a vehicle to—

(A) transmit commands to the vehicle;

(B) alter vehicle software or configuration;

(C) enable, disable, immobilize, limit, or materially affect vehicle operation;

(D) access vehicle sensors, microphones, cameras, location systems, or stored information;

(E) install, remove, or modify software;

(F) alter propulsion, braking, steering, charging, starting, locking, or other vehicle functions; or

(G) otherwise exercise control over a vehicle or a component thereof.

(4) ESSENTIAL VEHICLE FUNCTION.

The term “essential vehicle function” means any function reasonably necessary to start, propel, steer, brake, refuel or recharge, secure, maintain, diagnose, or otherwise operate a motor vehicle for ordinary transportation.

(5) VEHICLE CONNECTIVITY SYSTEM.

The term “vehicle connectivity system” means hardware or software installed in or on a connected vehicle that directly enables the transmission, receipt, conversion, or processing of radio-frequency or other electronic communications between the vehicle and an external system or device.

(6) VEHICLE CONNECTIVITY SYSTEM HARDWARE.

The term includes—

(A) microcontrollers;

(B) microcomputers and communication modules;

(C) systems on a chip;

(D) networking or telematics control units;

(E) cellular modems and modules;

(F) Wi-Fi modules;

(G) Bluetooth modules;

(H) satellite communication systems;

(I) wireless communication modules;

(J) external antennas;

(K) digital signal processors;

(L) field-programmable gate arrays;

(M) electronic systems integrated into a battery or battery-management system that permit external monitoring, management, security control, or communication; and

(N) any substantially similar device capable of facilitating communication between the vehicle and a remote system.

(7) COVERED ENTITY.

The term “covered entity” means—

(A) a motor vehicle manufacturer;

(B) software developer;

(C) hardware manufacturer or supplier;

(D) telecommunications provider;

(E) cloud-computing or data-hosting provider;

(F) dealership;

(G) repair facility;

(H) data broker;

(I) insurance company;

(J) financial institution or vehicle lender;

(K) Federal department or agency;

(L) Federal contractor;

(M) State, local, or Tribal governmental entity to the extent permitted by Federal law; or

(N) any other person or entity obtaining or exercising access to vehicle telemetry or remote vehicle functions.

No covered entity shall be excluded from the requirements of this Act because the entity is organized under the laws of, headquartered in, owned by, or controlled by a person in the United States.

SEC. 4. UNIFORM PROHIBITION AND VEHICLE AUTONOMY REQUIREMENTS.

(a) APPLICATION WITHOUT REGARD TO COUNTRY OF ORIGIN.

The requirements and prohibitions established under this Act shall apply uniformly to every covered vehicle, covered software item, connected vehicle hardware item, manufacturer, developer, supplier, and covered entity without regard to—

- (1) country of manufacture;
- (2) country of assembly;
- (3) country of software development;
- (4) country of hardware manufacture;
- (5) nationality of the manufacturer or developer;
- (6) location of the principal place of business of the manufacturer or developer; or
- (7) whether the manufacturer, developer, supplier, or person accessing the system is a domestic or foreign person.

A motor vehicle manufactured in the United States shall be subject to the same technical restrictions and requirements as a motor vehicle imported into the United States.

(b) PROHIBITED VEHICLE TELEMETRY.

On and after the applicable effective date, no person may import, manufacture, sell, resell, or introduce into interstate commerce in the United States a new motor vehicle containing a system designed to automatically transmit vehicle telemetry to a manufacturer, data center, laboratory, service provider, government entity, insurer, data broker, or other remote recipient unless—

- (1) the transmission is strictly necessary to provide a specific function knowingly requested by the vehicle owner or operator;
- (2) the owner or operator has provided affirmative and informed consent;
- (3) the vehicle remains capable of its essential vehicle functions if the owner refuses or later withdraws such consent; and
- (4) the system does not transmit information materially exceeding the information necessary to perform the specific function authorized by the owner or operator.

(c) NO CONDITIONING OF BASIC VEHICLE OPERATION.

A manufacturer or other covered entity may not condition an essential vehicle function upon—

- (1) continuous internet connectivity;
- (2) cellular connectivity;
- (3) satellite connectivity;
- (4) communication with a manufacturer-controlled server;
- (5) communication with a cloud-computing platform;
- (6) creation or continued maintenance of a manufacturer account;
- (7) acceptance of vehicle telemetry unrelated to the essential vehicle function;
- (8) payment of a recurring subscription fee for a function physically incorporated into the vehicle and necessary for ordinary operation; or
- (9) continued availability of infrastructure controlled by the manufacturer or another remote entity.

(d) REMOTE DISABLEMENT AND CONTROL.

Except as expressly authorized under this Act, no covered vehicle sold in the United States may contain hardware or software that permits a manufacturer, service provider, government agency, contractor, lender, insurer, telecommunications provider, or other remote entity to—

- (1) disable the vehicle;
- (2) prevent the vehicle from starting;
- (3) materially reduce propulsion capability;
- (4) remotely apply or interfere with braking;
- (5) remotely alter steering;
- (6) remotely restrict the geographic area in which the vehicle may operate;
- (7) remotely restrict vehicle operation based upon an external database or remote command;
- (8) remotely assume operational control of the vehicle; or

(9) otherwise render an otherwise mechanically operable vehicle unavailable for transportation.

(e) EMERGENCY AND INFRASTRUCTURE RESILIENCE.

Every covered vehicle shall be designed so that failure or unavailability of—

(1) cellular service;

(2) internet service;

(3) satellite communication;

(4) manufacturer servers;

(5) cloud-computing infrastructure;

(6) remote authentication services;

(7) subscription-management services; or

(8) any substantially similar external communications infrastructure,

does not prevent the owner or lawful operator from starting and operating the vehicle through its essential vehicle functions.

(f) GOVERNMENT ACCESS.

Except pursuant to a warrant issued upon probable cause, a court order satisfying applicable constitutional requirements, or an immediate emergency involving a specific and articulable threat of death or serious bodily injury, no Federal agency or Federal contractor may compel, request, purchase, obtain, or access nonpublic vehicle telemetry concerning an identifiable privately owned vehicle or its occupants.

Nothing in this subsection shall be interpreted to create independent authority for governmental access that would otherwise be prohibited by the Constitution or laws of the United States.

No government agency may require a manufacturer to maintain a remote-access, remote-disablement, location-tracking, or other technical capability that would otherwise be prohibited under this Act solely for the purpose of facilitating future government access.

(g) PROHIBITION ON CIRCUMVENTION.

The prohibitions of this Act shall apply to covered vehicles, software, hardware, services, or transactions that are renamed, rebranded, restructured, remotely activated, subscription-enabled, installed after sale, or otherwise altered for the purpose or effect of circumventing this Act.

(h) OWNER CONTROL.

The lawful owner of a motor vehicle shall have the right to disable any nonessential vehicle connectivity system without—

- (1) disabling an essential vehicle function;
- (2) voiding the vehicle warranty with respect to an unrelated component;
- (3) generating a persistent warning unrelated to vehicle safety;
- (4) preventing ordinary diagnosis or repair of the vehicle;
- (5) preventing registration or lawful operation of the vehicle; or
- (6) imposing a fee or subscription requirement.

A manufacturer shall provide a reasonably accessible means of disabling such connectivity.

SEC. 5. DECLARATION OF CONFORMITY.

Before importing, manufacturing, selling, or introducing a covered vehicle into interstate commerce in the United States, the manufacturer or importer shall submit a declaration of conformity certifying that—

- (1) the vehicle complies with this Act;
- (2) the vehicle does not contain a prohibited remote-disablement or remote-control capability;
- (3) essential vehicle functions remain operational without continuous external connectivity;
- (4) vehicle telemetry is limited to communications permitted under this Act;
- (5) the vehicle owner can disable nonessential external communications;
- (6) no undisclosed remote access mechanism, telecommunications pathway, or telemetry capability is incorporated into the vehicle; and
- (7) the manufacturer has accurately disclosed all external communication capabilities incorporated into the vehicle.

SEC. 6. INDEPENDENT TESTING AND VERIFICATION.

The Secretary shall establish procedures for independent technical verification of declarations of conformity.

Such verification may include laboratory examination, software analysis, network traffic analysis, hardware inspection, penetration testing, and testing of a vehicle while disconnected from all external communications networks.

Manufacturers shall provide sufficient technical information to an accredited independent testing laboratory to determine whether a vehicle complies with this Act.

No manufacturer may knowingly conceal an undocumented communications pathway, remote command capability, telemetry function, or other covered functionality from an accredited laboratory or the Secretary.

SEC. 7. CIVIL PENALTIES.

The Secretary shall assess a civil penalty for each transaction constituting a violation of this Act in an amount not less than the greater of—

- (1) \$1,500,000; or
- (2) five times the value of the transaction.

For a continuing violation, each day on which the violation continues shall constitute a separate violation.

For purposes of this section, each knowing undisclosed activation, collection, transmission, sale, disclosure, or provision of access to prohibited vehicle telemetry may constitute a separate violation.

SEC. 8. PRIVATE VEHICLE OWNERS.

Nothing in this Act shall prohibit a lawful vehicle owner from voluntarily—

- (1) installing communications equipment;
- (2) using navigation or emergency communications services;
- (3) transmitting vehicle information to a repair facility;
- (4) participating in a voluntary usage-based insurance program;
- (5) installing aftermarket connected-vehicle equipment; or
- (6) otherwise transmitting information from the owner's vehicle,

provided that such activity is knowingly initiated or authorized by the vehicle owner and does not establish an undisclosed means of third-party control.

SEC. 9. SAFETY AND EMERGENCY COMMUNICATIONS.

Nothing in this Act shall prohibit a communications system used solely for an immediate safety function, including an emergency communication knowingly initiated by an occupant or an automatic emergency communication triggered by a collision or comparable event presenting a substantial likelihood of death or serious bodily injury.

Any such system shall be technically limited, to the greatest extent practicable, to the information and duration reasonably necessary to address the immediate emergency.

The existence of a permitted emergency communication system shall not authorize continuous location tracking, continuous telemetry, remote vehicle disablement, or unrelated data collection.

SEC. 10. NO GENERAL GOVERNMENT BACKDOOR.

Nothing in this Act shall be construed to authorize the Federal Government to require the installation or retention of any—

- (1) remote vehicle disablement mechanism;
- (2) remote vehicle control mechanism;
- (3) continuous vehicle-location reporting mechanism;
- (4) government-access interface;
- (5) encryption backdoor;
- (6) remote authentication mechanism capable of preventing ordinary operation of a privately owned vehicle; or
- (7) other technical capability principally intended to permit future remote surveillance or control.

SEC. 11. REPORTS TO CONGRESS.

Not later than one year after enactment, and annually thereafter, the Secretary shall submit to Congress a report describing—

- (1) enforcement actions taken under this Act;
- (2) compliance rates among domestic and foreign manufacturers;
- (3) violations involving undisclosed telemetry;
- (4) violations involving unauthorized remote access or control;

(5) penalties assessed;

(6) identified cybersecurity vulnerabilities;

(7) the resilience of covered vehicles during communications and infrastructure outages;

(8) any attempts by domestic or foreign manufacturers or government entities to circumvent the requirements of this Act; and

(9) recommendations for further protecting the transportation autonomy, privacy, security, and freedom of movement of the American people.

SEC. 12. UNIFORM APPLICATION.

The Secretary shall administer this Act without preference for or discrimination against a manufacturer based solely upon the manufacturer's domestic or foreign status.

Compliance shall be determined according to the technical capabilities, software, hardware, data practices, remote-access capabilities, and communications architecture of the vehicle.

For purposes of protecting the American people, substantially similar technological capabilities shall be subject to substantially similar restrictions regardless of who owns, manufactures, operates, or seeks access to those capabilities.

SEC. 13. RULE OF CONSTRUCTION REGARDING OWNERSHIP.

Nothing in this Act shall be construed to diminish the traditional incidents of ownership of a motor vehicle.

The purchase of a motor vehicle shall not, merely because the vehicle incorporates software, convert the owner's possession and use of the vehicle into a revocable license from the manufacturer.

Except for functions expressly and knowingly obtained by subscription, the termination of a manufacturer's network, server, software service, business operations, or support for a vehicle shall not be designed to render the vehicle's essential vehicle functions inoperable.

SEC. 14. SEVERABILITY.

If any provision of this Act, or the application of such provision to any person or circumstance, is held invalid, the remainder of this Act and the application of the remaining provisions to any other person or circumstance shall not be affected.