SECOND REGULAR SESSION

HOUSE BILL NO. 1415

102ND GENERAL ASSEMBLY

INTRODUCED BY REPRESENTATIVE STACY.

4080H.01I DANA RADEMAN MILLER, Chief Clerk

AN ACT

To amend chapter 542, RSMo, by adding thereto ten new sections relating to unmanned aerial systems, with penalty provisions.

Be it enacted by the General Assembly of the state of Missouri, as follows:

Section A. Chapter 542, RSMo, is amended by adding thereto ten new sections, to be known as sections 542.550, 542.552, 542.554, 542.556, 542.558, 542.560, 542.562, 542.564, 542.566, and 542.568, to read as follows:

542.550. 1. Sections 542.550 to 542.568 shall be known and may be cited as "The Unmanned Aerial Systems Security Act of 2024".

542.552. 1. For the purposes of sections 542.550 to 542.568, the following terms mean:

(1) "Country of concern", the People's Republic of China, the Russian Federation, the Islamic Republic of Iran, the Democratic People's Republic of Korea, the Republic of Cuba, the Venezuelan regime of Nicolás Maduro, or the Syrian Arab Republic, including any agent of or any other entity under significant control of such foreign country of concern, or any other entity deemed by the governor in consultation with appropriate federal and state officials;

(2) "Critical component", a drone component related to flight controllers; radio; data transmission devices; cameras; gimbals; ground control systems; operating software, including cell phone or tablet applications, but not cell phone or tablet operating systems; network connectivity; or data storage. The term "critical component" shall not mean passive electronics such as resistors and non-data transmitting motors, batteries, and wiring;

EXPLANATION — Matter enclosed in bold-faced brackets **[**~~thus~~**]** in the above bill is not enacted and is intended to be omitted from the law. Matter in **bold-face** type in the above bill is proposed language.

(3) "Critical infrastructure", systems and assets, whether physical or virtual, so vital to the state of Missouri or the United States of America that the incapacity or destruction of such systems and assets would have a debilitating impact on state or national security, state or national economic security, state or national public health, or any combination of those matters. Critical infrastructure may be publicly or privately owned, and includes but is not limited to:

(a) Gas and oil production, storage, or delivery systems;

(b) Water supply, refinement, storage, or delivery systems;

(c) Telecommunications networks;

(d) Electrical power delivery systems;

(e) Emergency services;

(f) Transportation systems and services; or

(g) Personal data or otherwise classified information storage systems, including cybersecurity;

(4) "Data", any information, document, media, or machine-readable material regardless of physical form or characteristics that is created or obtained by a government agency in the course of official agency business;

(5) "Drone", an unmanned aircraft, watercraft, or ground vehicle or a robotic device that:

(a) Is controlled remotely by a human operator; or

(b) Operates autonomously through computer software or other programming;

(6) "Flight mapping software", any program or ground control system that allows for the user to:

(a) Input a set of coordinates or locations to which the drone will autonomously fly to in a predetermined flight pattern; or

(b) Control the flight path or destination of the drone from any device other than a dedicated handheld controller within sight of the drone;

(7) "Geofence", a virtual geographic boundary defined by global positioning system (GPS), radio frequency identification (RFID), or some other location positioning technology, created to prevent the use of drone devices within a restricted geographic area;

(8) "Government agency", any state, county, local, or municipal government entity or any unit of government created or established by law that uses a drone for any purpose;

(9) "Instructional technology", an interactive device used by a school that assists in instructing a class or a group of students and includes the necessary hardware and

software to operate the interactive device. The term also includes support systems in which an interactive device may mount and is not required to be affixed to the facilities;

(10) "Open data", data which are structured in a way that enables the data to be fully discoverable and usable by the public. The term does not include data that are restricted from public disclosure based on federal or state laws and regulations including, but not limited to, those related to privacy, confidentiality, security, personal health, business or trade secret information, and exemptions from state public records laws or data for which a government agency is statutorily authorized to assess a fee for its distribution;

(11) "Research and accountability purposes", a drone used in direct support of research on drone hardware, operating systems, software, communications systems and protocols, components, and data practices for the purpose of understanding the existence and extent of potential threats and vulnerabilities, and mitigations thereof. This research shall be conducted at the direction of a state government agency or a federal agency or a party contracted by a state government agency or federal agency to conduct the research;

(12) "School", an organization of students for instructional purposes on an elementary, secondary, or post-secondary level authorized under rules of the department of elementary and secondary education or the department of higher education and workforce development;

(13) "Sensitive location", a location in Missouri where drone usage is prohibited and that is required to be geofenced by companies that provide flight mapping software in order to prevent unauthorized use of drones. These locations shall include military locations, power stations, critical infrastructure, and other locations determined to be sensitive by the department of transportation in consultation with relevant state and federal authorities.

542.554. A government agency shall only use a drone from a manufacturer that meets the minimum security requirements specified in sections 542.550 to 542.568. A manufacturer that meets such requirements is deemed an approved manufacturer for the given tier as specified in section 542.556. Notwithstanding a manufacturer's designation as an approved manufacturer, the government agency is still required to ensure that the drone it intends to use complies with all applicable provisions of this rule.

542.556. 1. Drones shall be classified as follows:

(1) "Tier one", a drone that does not collect, transmit, or receive data during flight. Examples of such drones include drones that navigate along pre-programmed

waypoints and tethered drones. A drone used by a school exclusively as instructional technology shall be classified as tier one drone usage;

(2) "Tier two", a drone that may collect, transmit, or receive only flight control data, excluding visual and auditory data; or

(3) "Tier three", a drone that may collect, transmit, or receive any data, including visual or auditory data.

2. (1) Drones used for research and accountability purposes shall be exempt from the requirements in sections 542.558, 542.562, and 542.564. If using otherwise prohibited drones for research and accountability purposes, a government agency shall weigh the goals of the research against the risk to networks and data.

(2) A government agency using otherwise prohibited drones under the exception established under subdivision (1) of this subsection shall provide written notice to the department of transportation of such use no later than thirty days prior to utilizing the exception. Such notice shall state the intended purpose, participants, and ultimate beneficiaries of the research.

(3) To the extent allowed by law and existing agreement between the parties to the research, the government agency conducting research under the exception established under subdivision (1) of this subsection shall, upon the request of the department, provide access to the research findings.

542.558. A government agency shall not purchase, acquire, or otherwise use a drone or any related services or equipment produced by a manufacturer domiciled in a country of concern or produced by a manufacturer the government agency reasonably believes to be owned or controlled, in whole or in part, by a country of concern or a company domiciled in a country of concern.

542.560. 1. A drone or its software in use by a government agency shall connect to the internet only for purposes of command and control, coordination, or other communication to ground control stations or systems related to the mission of the drone. If connecting to the internet under this section, a government agency shall:

(1) Require the command and control, coordination, or other ground control stations or systems to be secured and monitored; or

(2) Require the command and control, coordination, or other ground control stations or systems to be isolated from networks where the data of a government agency is held.

2. (1) A drone or its software in use by a government agency shall connect to a computer or the network of a government agency only if:

(a) The drone or its software is isolated in a way that prevents access to the internet and any network where the data of a government agency is held;

(b) The drone or its software uses removable memory to connect to a computer or network that is isolated in a way that prevents access to a network where the data of a government agency is held; and

(2) Any transfer of data between an isolated network described in paragraphs (a) or (b) of subdivision 1 of this subsection and a network where the data of a government agency is held shall require:

(a) An initial scan for malicious code using antivirus or anti-malware software on the computer that connected directly or indirectly to the drone;

(b) The use of antivirus and anti-malware software during data transfer; and

(c) A scan for malicious code of the destination of the transferred data using antivirus and anti-malware software.

3. A drone or its software in use by a government agency shall not connect with a telephone, tablet, or other mobile device issued by a government agency or that connects to a government agency network. Government agency devices that are solely used for the command and control, coordination, or other communication to ground control stations or systems related to the mission of the drones that do not connect to the government agency's network may be used.

4. A drone or its software in use by a government agency shall be used in compliance with all other applicable data standards as required by law and the government agency's own policy and procedure.

542.562. A drone or any related services or equipment used in accordance with tier two, as defined in section 542.556, shall, in addition to the requirements in sections 542.558 and 542.560, meet the following minimum security requirements:

(1) Regardless of whether the government agency is a "government agency" as defined in subdivision (8) of section 542.552, the government agency shall comply with the portions of sections 542.550 to 542.568 that would by their nature be applicable to drone use, its software, or any related services or interaction with any data originating from the drone or its use;

(2) All communication to and from a drone shall utilize a Federal Information Process Standard (FIPS) 140-2 compliant encryption algorithm; and

(3) Critical components shall not be produced by a manufacturer domiciled in, or produced by a manufacturer the government agency believes to be owned, controlled by, or otherwise connected to, a country of concern.

542.564. A drone or any related services or equipment used in accordance with tier three as defined in section 542.556, shall, in addition to the requirements of sections 542.558, 542.560, and 542.562, meet the following minimum security requirements:

(1) Data storage shall be restricted to the geographic location of the United States; and

(2) Remote access to data storage, other than open data, from outside the United States shall be prohibited unless approved in writing by the government agency head or his or her designee.

542.566. Subject to appropriation, any department currently using a drone that does not meet the minimum requirements for that drone's usage tier may request a reimbursement up to the cost of acquiring a drone that meets the minimum requirements for that drone's usage tier from the state treasurer, provided the request includes purchase orders and a statement describing the drone's usage and necessity.

542.568. 1. The department of transportation, in consultation with other state, local, and federal authorities, shall identify the geographic coordinates of sensitive installations within the state of Missouri for the purpose of prohibiting drone usage over sensitive locations.

2. (1) Any provider of flight mapping software or any other program for operating a drone shall geofence the state's sensitive locations to prevent the flight of any drone over the state's sensitive locations.

(2) Drones used by law enforcement agencies shall be exempt from the usage restrictions of subdivision 1 of this subsection.

3. It shall be a class B misdemeanor for a provider of flight mapping software to allow a user to fly a drone over a sensitive location unless the user is a law enforcement agency or officer.

4. (1) It shall be a class B misdemeanor for a user of a drone that does not have flight mapping software to fly such a drone over a sensitive location.

(2) Law enforcement officers are exempt from the usage restrictions of subdivision (1) of this subsection.

(3) Individuals who have the permission of the authority in charge of the sensitive location to operate a drone in, on, or above the sensitive location are exempt from the usage restrictions of subdivision (1) of this subsection.

✓