SB3729

LRB10339070AWJ69207b

103RD GENERAL ASSEMBLY

State of Illinois

2023 and 2024

SB3729

Introduced 2/9/2024, by Sen. Jason Plummer

SYNOPSIS AS INTRODUCED:

New Act
30 ILCS 105/5.1015 new

Creates the Unmanned Aerial Systems Security Act. Provides that a government agency may use a drone only if the manufacturer of the drone meets the minimum security requirements specified in the Act. Prohibits a government agency from purchasing, acquiring, or otherwise using a drone or any related services or equipment produced by (i) a manufacturer domiciled in a country of concern or (ii) a manufacturer the government agency reasonably believes to be owned or controlled, in whole or in part, by a country of concern or by a company domiciled in a country of concern. Classifies 3 different tiers of drones, and specifies restrictions for each tier level. Requires, subject to appropriation, a government agency using a drone on January 1, 2025 that does not meet the minimum requirements for that drone's usage tier to receive a reimbursement from the Unmanned Aerial Systems Security Reimbursement Fund up to the cost of acquiring a drone that meets the minimum requirements for that drone's usage tier if specified requirements are met. Requires the Department of Transportation to identify the geographic coordinates of sensitive installations within Illinois for the purpose of prohibiting drone usage over sensitive locations. Requires a provider of flight mapping software or other program for operating a drone to geofence Illinois' sensitive locations to prevent the flight of a drone over Illinois' sensitive locations. Provides for criminal penalties for a provider of flight mapping software to allow a user to fly a drone over a sensitive location, except if the user is a law enforcement agency or officer, and for a user of a drone not using flight mapping software to fly a drone over a sensitive location. Limits the concurrent exercise of home rule powers. Contains a severability clause. Amends the State Finance Act to create the Unmanned Aerial Systems Security Reimbursement Fund. Effective January 1, 2025.

LRB103 39070 AWJ 69207 b

A BILL FOR

AN ACT concerning government.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 1. Short title. This Act may be cited as the Unmanned Aerial Systems Security Act.

Section 5. Purpose. The purpose of this Act is to prohibit State and local government procurement of unmanned aerial systems from countries of concern in order to protect State critical infrastructure and data security and to regulate the operation of unmanned aerial systems near military installations, power stations, and other sensitive locations.

Section 10. Definitions. As used in this Act:

"Country of concern" means 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 an agent of or any other entity under significant control of any of those countries, or any other entity deemed to be a country of concern by the Governor in consultation with Illinois Emergency Management Agency and Office of Homeland Security.

"Critical component" means 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. "Critical component" does not include passive electronics, such as resistors, or nondata transmitting motors, batteries, or wiring.

"Critical infrastructure" means a system or asset, whether physical or virtual, that is so vital to Illinois or the United States of America that the incapacity or destruction of the system and asset 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" includes, but is not limited to, publicly or privately owned systems, including:

(1) gas and oil production, storage, or delivery systems;

(2) water supply, refinement, storage, or delivery systems;

(3) telecommunications networks;

(4) electrical power delivery systems;

(5) emergency services;

(6) transportation systems and services; or

(7) personal data or otherwise classified information storage systems, including cybersecurity.

"Data" means information or document-readable,

media-readable, 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.

"Drone" means an unmanned aircraft, watercraft, or ground vehicle or a robotic device that:

(1) is controlled remotely by a human operator; or

(2) operates autonomously through computer software or other programming.

"Flight mapping software" means a program or ground control system that allows the user to:

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

(2) control the flight path or destination of the drone from any device other than a dedicated handheld controller within sight of the drone.

"Geofence" means a virtual geographic boundary defined by global positioning system, radio frequency identification, or some other location positioning technology created to prevent the use of drone devices within a restricted geographic area.

"Government agency" means a State government entity or a unit of local government created or established by law.

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

to operate the interactive device. "Instructional technology" includes a support system in which an interactive device may mount whether or not it is affixed to the facility.

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

"Research and accountability purposes" means activities that are (i) used in direct support of research concerning 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 thereto and (ii) conducted at the direction of a State government agency, a federal agency, or a party contracted by a State government agency or federal agency to conduct the research.

"School" means an organization of students for instructional purposes on an elementary, middle, or junior high school, secondary or high school, or any other public school level, including colleges and universities, authorized under rules of the State Board of Education, the State Board of

Higher Education, or the Illinois Community College Board.

"Sensitive location" means a location in Illinois where drone usage is prohibited and which must be geofenced by companies that provide flight-mapping software in order to prevent unauthorized use of drones. "Sensitive location" includes 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.

Section 15. Approved manufacturers. A government agency may use a drone only if that drone is produced by a manufacturer that meets the minimum security requirements specified in this Act. A manufacturer that meets such requirements is deemed an approved manufacturer for the given tier as specified in Section 20. 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 Act.

Section 20. Tiers; research and accountability purposes exception.

(a) Tier 1: a drone that does not collect, transmit, or receive data during flight, such as drones that navigate along pre-programmed waypoints, tethered drones, or drones used by a

school exclusively as instructional technology.

(b) Tier 2: a drone that may collect, transmit, or receive only flight control data, excluding visual and auditory data.

(c) Tier 3: a drone that may collect, transmit, or receive data, including visual and auditory data.

(d) Research and accountability purposes exception.

(1) Drones used for research and accountability purposes are exempt from the requirements in Sections 25, 35, and 40. If using otherwise prohibited drones for research and accountability purposes, the government agency must weigh the goals of the research against the risk to networks and data.

(2) A government agency using otherwise prohibited drones under this exception must provide written notice to the Illinois Emergency Management Agency and Office of Homeland Security of such use via email no later than 30 days prior to using the exception. Such notice must 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 this exception must, upon the request of the Illinois Emergency Management Agency and Office of Homeland Security, provide access to the research findings.

Section 25. Countries of concern. A government agency may not purchase, acquire, or otherwise use a drone or any related services or equipment produced by (i) a manufacturer domiciled in a country of concern or (ii) a manufacturer that the government agency reasonably believes to be owned or controlled, in whole or in part, by a country of concern or by a company domiciled in a country of concern.

Section 30. Tier 1 restrictions. A drone or its software in use by a government agency:

(1) may only connect to the Internet 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 paragraph, a government agency shall:

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

(B) 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, such as air-gapping;

(2) may only connect to a computer or the network of a government agency if:

(A) a drone or its software is isolated in a way that prevents access to the Internet and a network

where the data of a government agency is held;

(B) a 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 or is held; and

(C) transfer of data between an isolated network described in subparagraphs (A) and (B) and a network where the data of a government agency is held requires:

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

(ii) the use of antivirus and anti-malware software during data transfer; and

(iii) a scan of the destination of the transferred data using antivirus and anti-malware software for malicious code;

(3) may not connect with a telephone, tablet, or other mobile device issued by a government agency 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; and

(4) shall be used in compliance with all other applicable data standards as required by law and the government agency's own policy and procedure.

Section 35. Tier 2 restrictions. A drone or any related services or equipment used in accordance with Tier 2 must, in addition to the requirements in Sections 25 and 30, meet the following minimum security requirements:

(1) A government agency must comply with the portions of this Act that would by their nature be applicable to drone use, its software, or any related services or interacting with data originating from the drone or its use.

(2) Communication to and from a drone shall utilize a Federal Information Process Standard 140-2-compliant encryption algorithm.

(3) Critical components may 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.

Section 40. Tier 3 restrictions. A drone or any related services or equipment used in accordance with Tier 3 must, in addition to the requirements in Sections 25, 30, and 35, be restricted to the geographic location of the United States. Remote access to data storage, other than open data, from

outside the United States is prohibited unless approved in writing by the government agency head or designee.

Section 45. Replacement cost reimbursement requests.

(a) Subject to appropriation, a government agency using a drone on January 1, 2025 that does not meet the minimum requirements for that drone's usage tier may request a reimbursement from the Unmanned Aerial Systems Security Reimbursement Fund, a special fund that is created in the State treasury, and, subject to appropriation and as directed by the Director of the Illinois Emergency Management Agency and Office of Homeland Security, up to the cost of acquiring a drone that meets the minimum requirements for that drone's usage tier if the request includes purchase orders and a statement describing the drone's usage and necessity and the request is submitted to the Director by April 1, 2025.

(b) The Illinois Emergency Management Agency and the Office of Homeland Security shall adopt rules to create a procedure for reimbursement requests under this Section.

Section 50. Sensitive location geofencing; penalties.

(a) The Department of Transportation, in consultation with other State, local, and federal authorities, shall identify the geographic coordinates of sensitive installations within Illinois for the purpose of prohibiting drone usage over sensitive locations.

(b) A provider of flight mapping software or other program for operating a drone shall geofence Illinois' sensitive locations to prevent the flight of a drone over Illinois' sensitive locations. Drones used by law enforcement agencies are exempt from this subsection.

(c) It shall be a Class A 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.

(d) It shall be a Class A misdemeanor for a user of a drone not using flight mapping software to fly a drone over a sensitive location, except this subsection does not apply to an individual that has the permission of the governmental agency in charge of the sensitive location to operate a drone in, on, or above the sensitive location or law enforcement officers.

Section 90. Home rule. A home rule unit may not regulate unmanned aerial systems in a manner inconsistent with this Act. This Act is a limitation under subsection (i) of Section 6 of Article VII of the Illinois Constitution on the concurrent exercise by home rule units of powers and functions exercised by the State.

Section 97. Severability. The provisions of this Act are severable under Section 1.31 of the Statute on Statutes.

Section 900. The State Finance Act is amended by adding Section 5.1015 as follows:

(30 ILCS 105/5.1015 new)

Sec. 5.1015. The Unmanned Aerial Systems Security Reimbursement Fund.

Section 999. Effective date. This Act takes effect January 1, 2025.