

104TH GENERAL ASSEMBLY**State of Illinois****2025 and 2026****SB2364**

Introduced 2/7/2025, by Sen. Jason Plummer

SYNOPSIS AS INTRODUCED:

New Act
30 ILCS 105/5.1030 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, 2026 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 that it is a Class A misdemeanor for (i) 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; or (ii) a user of a drone not using flight mapping software to fly a drone over a sensitive location without permission from the governmental agency in charge of the 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, 2026.

LRB104 03800 BDA 13824 b

1 AN ACT concerning government.

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

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

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

12 Section 10. Definitions. As used in this Act:

13 "Country of concern" means the People's Republic of China,
14 the Russian Federation, the Islamic Republic of Iran, the
15 Democratic People's Republic of Korea, the Republic of Cuba,
16 the Venezuelan regime of Nicolás Maduro, or the Syrian Arab
17 Republic, including an agent of or any other entity under
18 significant control of any of those countries, or any other
19 entity deemed to be a country of concern by the Governor in
20 consultation with Illinois Emergency Management Agency and
21 Office of Homeland Security.

22 "Critical component" means a drone component related to

1 flight controllers, radio, data transmission devices, cameras,
2 gimbals, ground control systems, operating software, including
3 cell phone or tablet applications, but not cell phone or
4 tablet operating systems, network connectivity, or data
5 storage. "Critical component" does not include passive
6 electronics, such as resistors, or nondata transmitting
7 motors, batteries, or wiring.

8 "Critical infrastructure" means a system or asset, whether
9 physical or virtual, that is so vital to Illinois or the United
10 States of America that the incapacity or destruction of the
11 system and asset would have a debilitating impact on State or
12 national security, State or national economic security, State
13 or national public health, or any combination of those
14 matters. "Critical infrastructure" includes, but is not
15 limited to, publicly or privately owned systems, including:

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

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

20 (3) telecommunications networks;

21 (4) electrical power delivery systems;

22 (5) emergency services;

23 (6) transportation systems and services; or

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

26 "Data" means information or document-readable,

1 media-readable, or machine-readable material, regardless of
2 physical form or characteristics, that is created or obtained
3 by a government agency in the course of official agency
4 business.

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

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

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

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

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

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

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

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

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

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

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

13 "Research and accountability purposes" means activities
14 that are (i) used in direct support of research concerning
15 drone hardware, operating systems, software, communications
16 systems and protocols, components, and data practices for the
17 purpose of understanding the existence and extent of potential
18 threats and vulnerabilities, and mitigations thereto and (ii)
19 conducted at the direction of a State government agency, a
20 federal agency, or a party contracted by a State government
21 agency or federal agency to conduct the research.

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

1 Higher Education, or the Illinois Community College Board.

2 "Sensitive location" means a location in Illinois where
3 drone usage is prohibited and which must be geofenced by
4 companies that provide flight-mapping software in order to
5 prevent unauthorized use of drones. "Sensitive location"
6 includes military locations, power stations, critical
7 infrastructure, and other locations determined to be sensitive
8 by the Department of Transportation in consultation with
9 relevant State and federal authorities.

10 Section 15. Approved manufacturers. A government agency
11 may use a drone only if that drone is produced by a
12 manufacturer that meets the minimum security requirements
13 specified in this Act. A manufacturer that meets such
14 requirements is deemed an approved manufacturer for the given
15 tier as specified in Section 20. Notwithstanding a
16 manufacturer's designation as an approved manufacturer, the
17 government agency is still required to ensure that the drone
18 it intends to use complies with all applicable provisions of
19 this Act.

20 Section 20. Tiers; research and accountability purposes
21 exception.

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

1 school exclusively as instructional technology.

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

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

6 (d) Research and accountability purposes exception.

7 (1) Drones used for research and accountability
8 purposes are exempt from the requirements in Sections 25,
9 35, and 40. If using otherwise prohibited drones for
10 research and accountability purposes, the government
11 agency must weigh the goals of the research against the
12 risk to networks and data.

13 (2) A government agency using otherwise prohibited
14 drones under this exception must provide written notice to
15 the Illinois Emergency Management Agency and Office of
16 Homeland Security of such use via email no later than 30
17 days prior to using the exception. Such notice must state
18 the intended purpose, participants, and ultimate
19 beneficiaries of the research.

20 (3) To the extent allowed by law and existing
21 agreement between the parties to the research, the
22 government agency conducting research under this exception
23 must, upon the request of the Illinois Emergency
24 Management Agency and Office of Homeland Security, provide
25 access to the research findings.

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

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

10 (1) may only connect to the Internet for purposes of
11 command and control, coordination, or other communication
12 to ground control stations or systems related to the
13 mission of the drone. If connecting to the Internet under
14 this paragraph, a government agency shall:

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

18 (B) require the command and control, coordination,
19 or other ground control stations or systems to be
20 isolated from networks where the data of a government
21 agency is held, such as air-gapping;

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

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

1 where the data of a government agency is held;

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

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

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

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

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

19 (3) may not connect with a telephone, tablet, or other
20 mobile device issued by a government agency that connects
21 to a government agency network. Government agency devices
22 that are solely used for the command and control,
23 coordination, or other communication to ground control
24 stations or systems related to the mission of the drones
25 that do not connect to the government agency's network may
26 be used; and

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

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

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

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

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

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

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

3 Section 45. Replacement cost reimbursement requests.

4 (a) Subject to appropriation, a government agency using a
5 drone on January 1, 2026 that does not meet the minimum
6 requirements for that drone's usage tier may request a
7 reimbursement from the Unmanned Aerial Systems Security
8 Reimbursement Fund, a special fund that is created in the
9 State treasury, and, subject to appropriation and as directed
10 by the Director of the Illinois Emergency Management Agency
11 and Office of Homeland Security, up to the cost of acquiring a
12 drone that meets the minimum requirements for that drone's
13 usage tier if the request includes purchase orders and a
14 statement describing the drone's usage and necessity and the
15 request is submitted to the Director by April 1, 2026.

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

19 Section 50. Sensitive location geofencing; penalties.

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

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

6 (c) It shall be a Class A misdemeanor for a provider of
7 flight mapping software to allow a user to fly a drone over a
8 sensitive location unless the user is a law enforcement agency
9 or officer.

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

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

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

1 Section 900. The State Finance Act is amended by adding
2 Section 5.1030 as follows:

3 (30 ILCS 105/5.1030 new)

4 Sec. 5.1030. The Unmanned Aerial Systems Security
5 Reimbursement Fund.

6 Section 999. Effective date. This Act takes effect January
7 1, 2026.