House Study Bill 704 - Introduced

HOUSE FILE _____
BY (PROPOSED COMMITTEE ON PUBLIC SAFETY BILL BY CHAIRPERSON THOMPSON)

A BILL FOR

An Act relating to the procurement and operation of drones, and providing penalties.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

Section 1. NEW SECTION. **29D.1 Definitions.**

For purposes of this chapter:

1. *"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 Nicolas Maduro, or the Syrian Arab Republic, including an agent of or an entity under significant control of such foreign country of concern, or an entity deemed a country of concern by the governor in consultation with appropriate federal and state officials.

2. *"Data"* means 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.

3. *"Department"* means the department of homeland security and emergency management.

4. *"Drone"* means an unmanned aircraft, watercraft, ground vehicle, or robotic device that is controlled remotely by a human operator or that operates autonomously through computer software or other programming. Drones shall be classified as follows:

a. "Tier one" means a drone that does not collect, transmit, or receive data during flight, such as a drone that navigates along preprogrammed waypoints or a tethered drone. A drone used by any school, including a postsecondary institution, exclusively as an interactive device for instructing a group of students is a tier one drone.

b. "Tier two" means a drone that can collect, transmit, or receive only flight control data, excluding visual and auditory data.

c. "Tier three" means a drone that can collect, transmit, or receive any data, including visual or auditory data.

5. *"Flight-mapping software"* means a program or ground control system that allows the user to do any of the following:

a. Input a set of coordinates or locations to which the

drone will autonomously fly in a predetermined flight pattern.

b. Control the flight path or destination of the drone from a device other than a dedicated handheld controller within sight of the drone.

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

7. *"Government agency"* means a state, county, or municipal government entity or any other unit of government in this state established pursuant to state or local law.

8. *"Open data"* means data structured in a way that enables the data to be fully discoverable and usable by the public. *"Open data"* does not include data 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.

9. *"Research and accountability purposes"* means drone use in direct support of research authorized by a state government agency or a federal agency on drone hardware, operating systems, software, communications systems and protocols, components, and data practices for the purpose of understanding the existence, extent, and mitigation of potential threats and vulnerabilities.

10. *"Sensitive location"* means a location in this state where drone usage is restricted as provided in section 29D.7, including all of the following:

a. Military locations.

b. Power stations.

c. Physical or virtual systems and assets, whether publicly or privately owned, the incapacity of which would debilitate state or national security, economic security, or public

health, including all of the following:

(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.

(7) Personal data or other classified information storage systems, including cybersecurity.

d. Other locations determined to be sensitive by the department of homeland security and emergency management in consultation with relevant state and federal authorities.

Sec. 2. NEW SECTION. **29D.2 Applicability.**

1. A government agency shall not use a drone unless it is manufactured by a manufacturer, and used in a manner, that meets the minimum security requirements of this chapter.

2. *a.* A government agency using a drone for research and accountability purposes is exempt from the requirements in sections 29D.3, 29D.5, and 29D.6. If using an otherwise prohibited drone for research and accountability purposes, a government agency shall weigh the goals of the research against the risk to networks and data.

b. A government agency using an otherwise prohibited drone under paragraph *"a"* shall provide written notice to the department of such use no later than thirty days prior to utilizing the exception, stating the intended purpose, participants, and ultimate beneficiaries of the research.

c. To the extent allowed by law and existing agreement between the parties to the research, the government agency conducting research under paragraph *"a"* shall, upon the request of the department, provide the department access to the research findings.

Sec. 3. NEW SECTION. **29D.3 Countries of concern.**

A government agency shall not purchase, acquire, or use a drone or related service or equipment produced by

a manufacturer domiciled in a country of concern or 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.

Sec. 4. NEW SECTION. **29D.4 Tier one prohibitions.**

1. This section applies to tier one drones.

2. A government agency shall not connect a drone or a drone's software to the internet unless it is for purposes of command and control, coordination, or other communication to ground control stations or systems related to the drone's mission. When connecting to the internet, a government agency shall require the command and control, coordination, or other ground control stations or systems to be one of the following:

a. Secured and monitored.

b. Isolated from networks where the data of a government agency is held.

3. *a.* A government agency shall not connect a drone or a drone's software to a computer or the network of a government agency unless any of the following conditions are met:

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

(2) The drone or the drone's 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.

b. When a government agency transfers data between an isolated network described in paragraph "*a*", subparagraph (1) or (2), and a network where the data of a government agency is held, the government agency shall do all of the following:

(1) Conduct an initial scan using antivirus or antimalware software for malicious code on the computer that connected directly or indirectly to the drone.

(2) Use antivirus and antimalware software during the data transfer.

(3) Scan the destination of the transferred data for malicious code using antivirus and antimalware software.

4. A government agency shall not connect a drone or a drone's software with a telephone, tablet, or other mobile device that was 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 drone that do not connect to the government agency's network may be used.

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

Sec. 5. NEW SECTION. **29D.5 Tier two prohibitions.**

1. This section applies to tier two drones.

2. A government agency using a drone or any related services or equipment shall, in addition to the requirements in sections 29D.3 and 29D.4, do all of the following:

a. Utilize an encryption algorithm that complies with federal information processing standard 140-2 for all communication to and from a drone.

b. Refrain from purchasing critical drone components, including components related to flight controllers, radio, data transmission devices, cameras, gimbals, ground control systems, operating software including cellular telephone or tablet applications but not operating systems, network connectivity, or data storage, that were 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. This paragraph does not prohibit purchase of passive electronics such as resistors and nondata transmitting motors, batteries, and wiring from 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.

Sec. 6. NEW SECTION. **29D.6 Tier three prohibitions.**

1. This section applies to tier three drones.

2. A government agency, when using a drone or any related services or equipment, shall, in addition to the requirements of sections 29D.3, 29D.4, and 29D.5, do all of the following:

a. Restrict data storage to the geographic location of the United States.

b. Remotely access data other than open data from outside the United States only with written approval from the government agency's top official or the official's designee.

Sec. 7. NEW SECTION. **29D.7 Sensitive location restrictions — geofencing — penalties.**

1. The department, in consultation with other state, local, and federal authorities, shall identify the geographic coordinates of sensitive installations within the state for the purpose of designating the installations as sensitive locations.

2. *a.* The user of a drone shall not fly the drone over a sensitive location unless the user is a law enforcement officer or the user is authorized by the authority in charge of the sensitive location.

b. A provider of flight-mapping software shall geofence the state's sensitive locations to prevent the flight of a drone over the sensitive locations unless the user is not prohibited under paragraph *"a"*.

3. A person who violates subsection 2 is guilty of a serious misdemeanor.

Sec. 8. TRANSITION PROVISIONS.

1. A government agency possessing a drone that does not meet the minimum requirements for the drone's usage tier under this Act shall make every effort, subject to available funding, to replace the noncompliant drone with a drone that meets the minimum requirements for that drone's usage tier or promptly cease to use the noncompliant drone. A government agency shall

not continue to possess or use a noncompliant drone after July 1, 2029.

2. A government agency continuing to use a drone that does not meet the minimum requirements for that drone's usage tier under this Act shall provide written notice to the department of homeland security and emergency management of such use no later than thirty days following the effective date of this Act and every six months thereafter until the government agency no longer possesses or utilizes a noncompliant drone.

EXPLANATION

The inclusion of this explanation does not constitute agreement with the explanation's substance by the members of the general assembly.

This bill requires that government agencies only use a drone that meets minimum security requirements unless the government agency uses the drone for research and accountability purposes and notifies the department of homeland security and emergency management (HSEMD) in writing.

The bill prohibits a government agency from purchasing, acquiring, or using a drone produced by a manufacturer domiciled in a country of concern, defined in the bill, or that a government agency reasonably believes to be owned or controlled by a country of concern or a company domiciled in a country of concern.

The bill requires a government agency using a tier one drone to follow certain precautions when connecting the drone to the internet, a computer, or a network. A government agency is prohibited from connecting a tier one drone or the drone's software to the internet unless it is for purposes of command and control, coordination, or other communication to ground control stations. The command and control, coordination, or other ground control systems to which a drone is connected must be secured and monitored or isolated from networks where the data of a government agency is held. When connecting a drone to a computer or network, the government agency must ensure that the drone is isolated in a way that prevents access to the

internet or a network where a government agency's data is held or that the computer or network to which the drone connects is isolated to prevent such access. When a government agency transfers data to a network where government data is held, the government agency must conduct scans for malicious code and use antivirus and antimalware software during the data transfer. The bill also prohibits a government agency from connecting a tier one drone or the drone's software with a telephone, tablet, or other mobile device that was issued by a government agency or that connects to a government agency network unless the device is used solely for command and control, coordination, or other communication to ground control stations and does not connect to a government agency network.

A government agency using a tier two drone must comply with all security requirements for a tier one drone, use an encryption algorithm that complies with federal standards for all communication to and from a drone, and refrain from purchasing critical drone components from a manufacturer owned, controlled by, or connected to a country of concern.

A government agency using a tier three drone must comply with all security requirements for tier one and two drones and store all data in the United States. A government agency must not use a tier three drone to remotely access data from outside the United States without written approval from the agency's top official.

The bill restricts drone usage over sensitive locations, defined in the bill. The bill prohibits a user of a drone from flying the drone over a sensitive location unless the user is a law enforcement officer or the user is authorized by the authority in charge of the sensitive location. A provider of flight-mapping software must geofence the state's sensitive locations. A violation of these provisions is a serious misdemeanor. A serious misdemeanor is punishable by confinement for no more than one year and a fine of at least $430 but not more than $2,560.

To continue using a noncompliant drone after the passage of the bill, an agency must provide written notice to HSEMD every six months about such use. A government agency must not use a noncompliant drone after July 1, 2029.