HOUSE BILL NO. 5330

December 02, 2025, Introduced by Reps. Robinson, Kelly, Martus, Mentzer, Harris, BeGole, Schriver, Woolford, Pavlov, Steckloff, T. Carter, Arbit, Frisbie, Hoadley, Bruck, Herzberg, Liberati, Meerman, Breen, Kunse, Thompson, Cavitt, Markkanen, Aragona and Bierlein and referred to Committee on Transportation and Infrastructure.

A bill to amend 2016 PA 436, entitled

"Unmanned aircraft systems act,"

(MCL 259.301 to 259.331) by adding section 16.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

Sec. 16. (1) Beginning 1 year after the effective date of the amendatory act that added this section, a public entity or a person contracting with a public entity shall not procure, purchase, operate, or deploy a small unmanned aircraft system unless the small unmanned aircraft system complies with the requirements of this section.

(2) All of the following requirements apply to small unmanned aircraft systems described in subsection (1):

(a) All video footage, photographs, telemetry data, and personally identifiable information including, but not limited to, names, addresses, and other identifying details, collected, transmitted, or stored must be collected, transmitted, or stored only within the United States and must be managed in compliance with federal and state privacy laws, cybersecurity standards, and guidelines issued by the Cybersecurity and Infrastructure Security Agency and the Federal Bureau of Investigation.

(b) Must use end-to-end encryption for data-at-rest and data-in-transit using AES-256 encryption and transport layer security protocols to prevent unauthorized access.

(c) Must operate on a secured, segmented network to mitigate cybersecurity risks.

(d) Must require multifactor authentication and role-based access controls to limit access.

(e) Must incorporate tamper-proof hardware to prevent unauthorized modifications.

(f) Must utilize automatic deletion policies ensuring data removal within 45 days unless otherwise specified by law enforcement or public safety agencies.

(g) Must incorporate real-time monitoring systems capable of detecting unauthorized access, cyber threats, or operational anomalies, with automated countermeasures deployed as necessary.

(3) A public entity or person contracting with a public entity using a small unmanned aircraft system must conduct security audits annually and obtain certifications demonstrating compliance with all of the following cybersecurity standards:

(a) The National Institute of Standards and Technology Cybersecurity Framework 2.0.

(b) ISO 27001.

(c) SOC 2.

(4) The department of state police shall establish regulations or guidance for implementing this section, including, but not limited to, all of the following:

(a) Required security assessments for all small unmanned aircraft systems.

(b) Privacy protection measures and compliance verification.

(c) Network security controls and intrusion detection standards.

(d) Cybersecurity training requirements for small unmanned aircraft system operators.

(e) Enforcement mechanisms ensuring that any small unmanned aircraft system that does not meet the requirements of this section is disqualified from use by a public entity or a person contracting with a public entity.

(5) As used in this section:

(a) "Public entity" means that term as defined in section 1 of 1968 PA 317, MCL 15.321.

(b) "Small unmanned aircraft system" means a powered aircraft that meets both of the following:

(*i*) Operates without direct human intervention from within or on the aircraft.

(*ii*) Has a total weight, including any attached or carried components, of less than 55 pounds.