State of Arkansas *As Engrossed: H2/25/25 H3/11/25*
95th General Assembly **A Bill**
Regular Session, 2025 HOUSE BILL 1549

By: Representative R. Scott Richardson
By: Senator J. Bryant

For An Act To Be Entitled

AN ACT TO CREATE THE ARKANSAS CYBERSECURITY ACT OF 2025; AND FOR OTHER PURPOSES.

Subtitle

TO CREATE THE ARKANSAS CYBERSECURITY ACT OF 2025.

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

SECTION 1. DO NOT CODIFY. Title.

This act shall be known and may be cited as the "Arkansas Cybersecurity Act of 2025".

SECTION 2. Arkansas Code Title 25, Chapter 4, is amended to add an additional section to read as follows:

25-4-130. State Cybersecurity Office — Duties and powers — Definitions.

(a) As used in this section:

(1) "Cybersecurity":

(A) Means the practice of protecting a system, network, device, and data from cyber threats, unauthorized access, and malicious activities; and

(B) Involves a combination of technologies, processes, policies, and practices designed to safeguard and ensure the confidentiality, integrity, and availability of digital assets;

(2) "Functional report" means the practice of aligning employees based on function, including without limitation cybersecurity function and

information security function, and including without limitation the following factors:

(A) Monitoring and responding to threats;

(B) Incident response and recovery;

(C) Vulnerability management;

(D) Security awareness training;

(E) Compliance and risk management; and

(F) Implementation and adherence to cybersecurity governance and standards;

(3) "Information security" means a practice or system that eliminates or reduces the risk of state information being maliciously or improperly accessed through physical or electronic means; and

(4) "State agency" means a department, agency, division, board, or commission within the executive branch of the state government.

(b) The State Cybersecurity Office shall:

(1) Be managed by the State Information Security Officer;

(2) Be responsible for directing and managing all functions related to state cybersecurity and information security for each state agency;

(3) Maximize state cybersecurity resources, including without limitation cybersecurity personnel;

(4) Establish cybersecurity governance policies, procedures, and standards to protect state information technology systems and infrastructure, including without limitation:

(A) Data classification and design controls;

(B) Cybersecurity and data breach notification;

(C) Detection, mitigation, and monitoring of cybersecurity threats;

(D) A cyber assessment program and remediation actions;

(E) Cybersecurity awareness and training;

(F) Enforcement and compliance, including without limitation:

(i) Creation of a procedure for auditing;

(ii) Implementation of a state incident response plan and incident response team;

(iii) Coordination with state and federal agencies, including without limitation service as the incident response coordinator;

(iv) Service as a cybersecurity resource for local, state, and federal agencies, utilities and other service providers, academic institutions, and nongovernmental organizations; and

(v) Audit of the compliance of each state agency with state and federal cybersecurity governance standards, policies, and procedures; and

(5)(A) Report the audit and enforcement findings of the State Cybersecurity Office in a closed meeting to the Joint Committee on Advanced Communications and Information Technology at least two (2) times per calendar year and at the call of the chair, as appropriate.

(B) The report under subdivision *(b)(5)(A)* of this section shall detail cyber assessment and remediation actions, department noncompliance, and other cybersecurity efforts that the State Cybersecurity Office determines are relevant.

(c) A state agency shall comply with the governance standards, policies, and procedures established by the State Cybersecurity Office under subdivision

(b)(4) of this section, except:

(1) The standards of a state agency may be more stringent than the statewide minimum standards, but in no case less than the minimum standards; and

(2) When federal standards apply that are stricter than the statewide minimums, the federal standards shall apply.

(d) The State Information Security Officer may create a Cybersecurity Governance Team to assist the State Cybersecurity Office in the development and administration of the State Cybersecurity Office's cybersecurity plan, standards, policies, and procedures.

(e)(1) Except as provided under subdivision (e)(2) of this section, cybersecurity personnel and personnel with job functions that relate to information security within each state agency shall functionally report to the State Cybersecurity Office for the purpose of implementing this section.

(2) The positions, funding, and daily management of cybersecurity personnel and personnel with job functions related to information security under subdivision (e)(1) of this section shall remain with each respective *state agency.*

(f) This section shall not be construed as requiring access to data that

is protected by state or federal law.

/s/R. Scott Richardson