

1 State of Arkansas
2 95th General Assembly
3 Regular Session, 2025
4

A Bill

HOUSE BILL 1549

5 By: Representative R. Scott Richardson
6 By: Senator J. Bryant
7

For An Act To Be Entitled

8
9 AN ACT TO CREATE THE ARKANSAS CYBERSECURITY ACT OF
10 2025; AND FOR OTHER PURPOSES.
11

Subtitle

12
13
14 TO CREATE THE ARKANSAS CYBERSECURITY ACT
15 OF 2025.
16

17 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF ARKANSAS:
18

19 SECTION 1. DO NOT CODIFY. Title.

20 This act shall be known and may be cited as the "Arkansas Cybersecurity
21 Act of 2025".
22

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

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

27 (a) As used in this section:

28 (1) "Cybersecurity":

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

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

35 (2) "Information security" means a practice or system that
36 eliminates or reduces the risk of state information being maliciously or



1 improperly accessed through physical or electronic means; and

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

4
 5 (b) The State Cybersecurity Office shall:

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

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

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

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

14 (A) Data classification and design controls;

15 (B) Cybersecurity and data breach notification;

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

18 (D) A cyber assessment program and remediation actions;

19 (E) Cybersecurity awareness and training;

20 (F) Enforcement and compliance, including without limitation
 21 a procedure for auditing;

22 (G) Implementation of a state incident response plan and
 23 incident response team;

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

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

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

31 (6)(A) Report its findings in a closed meeting to the Joint
 32 Committee on Advanced Communications and Information Technology at least two
 33 (2) times per calendar year.

34 (B) The report under subdivision (b)(6)(A) of this section
 35 shall detail cyber assessment and remediation actions, department
 36 noncompliance, and other cybersecurity efforts that the State Cybersecurity

1 Office determines are relevant.

2 (c) A state agency shall comply with the governance standards, policies,
3 and procedures established by the State Cybersecurity Office under subdivision
4 (b)(4) of this section.

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

9 (e)(1) Except as provided under subdivision (e)(2) of this section,
10 cybersecurity personnel and personnel with job functions related to information
11 security within each state agency shall functionally report to the State
12 Cybersecurity Office beginning on the effective date of this act.

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

17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36