

IN THE HOUSE OF REPRESENTATIVES

HOUSE BILL NO. 4

BY STATE AFFAIRS COMMITTEE

AN ACT

1 RELATING TO INFORMATION TECHNOLOGY SERVICES AND CYBERSECURITY; AMENDING  
2 SECTION 67-827A, IDAHO CODE, TO REVISE PROVISIONS REGARDING POWERS AND  
3 DUTIES, TO REQUIRE THE IMPLEMENTATION OF CYBERSECURITY BEST PRACTICES,  
4 TO REQUIRE CERTAIN USE OF MULTIFACTOR IDENTIFICATION, AND TO MAKE TECH-  
5 NICAL CORRECTIONS; AMENDING SECTION 67-831, IDAHO CODE, TO DEFINE A  
6 TERM AND TO MAKE TECHNICAL CORRECTIONS; AMENDING CHAPTER 23, TITLE  
7 67, IDAHO CODE, BY THE ADDITION OF A NEW SECTION 67-2362, IDAHO CODE,  
8 TO PROVIDE FOR THE USE OF MULTIFACTOR IDENTIFICATION BY THE LEGISLA-  
9 TIVE BRANCH, JUDICIAL BRANCH, AND ELECTED CONSTITUTIONAL OFFICERS; AND  
10 DECLARING AN EMERGENCY AND PROVIDING AN EFFECTIVE DATE.  
11

12 Be It Enacted by the Legislature of the State of Idaho:

13 SECTION 1. That Section 67-827A, Idaho Code, be, and the same is hereby  
14 amended to read as follows:

15 67-827A. POWERS AND DUTIES. The office of information technology ser-  
16 vices is hereby authorized and directed:

17 (1) (a) (i) To control and approve the acquisition and installa-  
18 tion of all telecommunications equipment and facilities for all  
19 departments and institutions of state government, except as pro-  
20 vided in subparagraphs (ii), (iii) and (iv) of this paragraph;

21 (ii) To ~~coordinate~~ direct the acquisition and installation of all  
22 telecommunications equipment and facilities for the institutions  
23 of higher education and the elected officers in the executive  
24 branch;

25 (iii) To ~~coordinate~~ direct the acquisition and installation of all  
26 telecommunications equipment and facilities for the legislative  
27 and judicial branches;

28 (iv) Provided however, that the acquisition and installation of  
29 all public safety and microwave equipment shall be under the con-  
30 trol of the military division. The military division is autho-  
31 rized to charge and receive payment for actual and necessary ex-  
32 penses incurred in providing services to any unit of state govern-  
33 ment under the provisions of this subparagraph.

34 (b) In approving or ~~coordinating~~ directing the acquisition or in-  
35 stallation of telecommunications equipment or facilities, the office  
36 shall first consult with and consider the recommendations and ad-  
37 vice of the directors or executive heads of the various departments  
38 or institutions. Any acquisition or installation of any telecommu-  
39 nications equipment or facilities that is contrary to the office's  
40 ~~recommendation~~, direction or is not in harmony with the state's overall  
41 plan for telecommunications and information sharing, shall be reported  
42 in writing to the governor and the legislature.

1 (2) To provide a system of telecommunications for all departments and  
 2 institutions of state government. Funds received pursuant to this subsec-  
 3 tion shall be appropriated for payment of telecommunications and telephone  
 4 charges incurred by the various agencies and institutions of state govern-  
 5 ment.

6 (3) To provide a means whereby political subdivisions of the state may  
 7 use the state telecommunications system, ~~upon~~ on such terms and under such  
 8 conditions as the office of information technology services may establish.

9 (4) To accept federal funds granted by congress or by executive order  
 10 for all or any of the purposes of this chapter, as well as gifts and donations  
 11 from individuals and private organizations or foundations.

12 (5) To oversee implementation of cybersecurity policies ~~to that~~ fos-  
 13 ter risk and cybersecurity management telecommunications and decision-mak-  
 14 ing with both internal and external organizational stakeholders.

15 (6) To ~~coordinate and~~ consult with and direct state agencies and offi-  
 16 cials regarding information security needs.

17 (7) To ~~coordinate with~~ direct state agencies and officials on penetra-  
 18 tion tests and vulnerability scans of state technology systems in order to  
 19 identify steps to mitigate identified risks.

20 (8) To ~~coordinate with~~ direct state agencies and officials to ensure  
 21 that state agencies implement mandatory education and training of state em-  
 22 ployees and provide guidance on appropriate levels of training for various  
 23 classifications of state employees.

24 (9) To ~~coordinate with~~ direct appropriate state agencies to create,  
 25 coordinate, publish, routinely update and market a statewide cybersecurity  
 26 website as an information repository for intelligence-sharing and cyberse-  
 27 curity best practices.

28 (10) To ensure that all state agencies implement and maintain cyberse-  
 29 curity best practices.

30 (11) To require all state agencies to implement and use multifactor  
 31 identification to access information technology devices or services, in-  
 32 cluding but not limited to local and remote network access to any email  
 33 accounts, cloud storage accounts, web applications, networks, databases, or  
 34 servers.

35 ~~(10)~~ (12) To coordinate public and private entities to develop, create  
 36 and promote statewide public outreach efforts to protect personal informa-  
 37 tion and sensitive data from cyber threats.

38 ~~(11)~~ (13) To promulgate and adopt reasonable rules for effecting the  
 39 purposes of this act pursuant to the provisions of chapter 52, title 67,  
 40 Idaho Code.

41 SECTION 2. That Section 67-831, Idaho Code, be, and the same is hereby  
 42 amended to read as follows:

43 67-831. DEFINITIONS. As used in this chapter:

44 (1) "Information technology" means all present and future forms of com-  
 45 puter hardware, computer software, and services used or required for auto-  
 46 mated data processing, computer-related office automation, or telecommuni-  
 47 cations.

1       (2) "Multifactor identification" means using two (2) or more different  
2 types of identification credentials to achieve authentication. Acceptable  
3 identification credentials include any two (2) or more of the following:

4       (a) Knowledge-based credentials that require a user to provide infor-  
5 mation that they know such as passwords or personal identification num-  
6 bers;

7       (b) Possession-based credentials that require an individual to have  
8 something specific in their possession such as security tokens, key  
9 fobs, SIM cards, or smartphone applications; or

10       (c) Inherence-based credentials that require user-specific biologi-  
11 cal traits to confirm identity for login, such as fingerprints or facial  
12 recognition.

13       ~~(2)~~ (3) "State agencies" means all state agencies or departments,  
14 boards, commissions, councils, and institutions of higher education but  
15 shall not include the elected constitutional officers and their staffs, the  
16 legislature and its staffs, or the judiciary.

17       ~~(3)~~ (4) "Telecommunications" means all present and future forms of  
18 hardware, software or services used or required for transmitting voice,  
19 data, video, or images over a distance.

20       SECTION 3. That Chapter 23, Title 67, Idaho Code, be, and the same is  
21 hereby amended by the addition thereto of a NEW SECTION, to be known and des-  
22 ignated as Section 67-2362, Idaho Code, and to read as follows:

23       67-2362. USE OF MULTIFACTOR IDENTIFICATION REQUIRED. (1) The legisla-  
24 tive branch and its staff, the judicial branch and its staff, and the elected  
25 constitutional officers and their staffs shall implement the use of multi-  
26 factor identification as that term is defined in section 67-831, Idaho Code.

27       (2) Multifactor identification shall be required to access informa-  
28 tion technology devices or services as those terms are described in section  
29 67-831, Idaho Code, including but not limited to local and remote network  
30 access to any email accounts, cloud storage accounts, web applications,  
31 networks, databases, or servers.

32       SECTION 4. An emergency existing therefor, which emergency is hereby  
33 declared to exist, this act shall be in full force and effect on and after  
34 July 1, 2025.