LEGISLATURE OF THE STATE OF IDAHO

Sixty-eighth Legislature First Regular Session - 2025

IN THE HOUSE OF REPRESENTATIVES

HOUSE BILL NO. 421

BY APPROPRIATIONS COMMITTEE

AN ACT

RELATING TO THE CYBERSECURITY AND RESILIENCY FUND; AMENDING CHAPTER 8, TITLE 67, IDAHO CODE, BY THE ADDITION OF A NEW SECTION 67-838, IDAHO CODE, TO PROVIDE FOR THE CYBERSECURITY AND RESILIENCY FUND; AND DECLARING AN EMERGENCY AND PROVIDING AN EFFECTIVE DATE.

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

SECTION 1. That Chapter 8, Title 67, Idaho Code, be, and the same is hereby amended by the addition thereto of a NEW SECTION, to be known and designated as Section 67-838, Idaho Code, and to read as follows:

67-838. CYBERSECURITY AND RESILIENCY FUND. (1) There is hereby created in the state treasury the cybersecurity and resiliency fund. The fund shall consist of moneys that may be provided by legislative appropriation or transfer. The state treasurer shall invest the idle moneys of the fund, and the interest earned on such investments shall be retained by the fund.

(2) All moneys now or hereafter in the cybersecurity and resiliency fund shall be used to address the state's ongoing needs for information technology infrastructure and cybersecurity technology.

(3) The office of information technology services shall create a five (5) year plan for replacement of information technology infrastructure and cybersecurity technology. Every year, the office of information technology services shall update the plan and submit it to the division of financial management as a part of the annual budget process. The office of information technology services shall also account for and provide information regarding any money spent from the fund during the previous fiscal year.

(4) For the purposes of this section:

(a) "Cybersecurity technology" means technology used to protect networks, devices, and data from unauthorized access or criminal use and includes network and data center security, endpoint security, cloud security, security information and event management, data protection and recovery, data encryption, identity protection, incident response, security awareness training and audits, penetration testing, technology resilience, and redundancy measures.

(b) "Information technology infrastructure" means network infrastructure and computers and storage, including desktops and laptops.

SECTION 2. An emergency existing therefor, which emergency is hereby declared to exist, this act shall be in full force and effect on and after July 1, 2025.