Date of Hearing: August 20, 2025

ASSEMBLY COMMITTEE ON APPROPRIATIONS
Buffy Wicks, Chair
SB 833 (McNerney) – As Amended July 17, 2025

Policy Committee: Privacy and Consumer Protection Vote: 15 - 0

Urgency: No State Mandated Local Program: No Reimbursable: No

SUMMARY:

This bill imposes oversight requirements on state agencies that operate covered artificial intelligence (AI) systems that affect the state's critical infrastructure.

"Covered AI system" means an AI system or automated decision system (ADS) that an operator uses to operate, manage, oversee, or control access to critical infrastructure.

"Critical infrastructure" means systems or assets so vital that their incapacity, unintended use, or destruction would have a debilitating impact on public health, safety, or economic security. Critical infrastructure includes but is not limited to the following sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, health care and public health, information technology, and nuclear reactors, among others.

Specifically, among other provisions, this bill:

1) Requires, on or after July 1, 2026, oversight personnel for an operator that deploys a covered AI system to establish an oversight mechanism to ensure a human monitors the AI system's operations in real time and reviews and approves any plan or action proposed by the covered AI system before execution, with specified exceptions.

2) Requires the Department of Technology (CDT) to develop a specialized training in AI safety protocols and risk management techniques to be given annually to oversight personnel.

3) Requires each operator of a covered AI system to designate at least one employee to serve as oversight personnel who is responsible for administering the human oversight mechanism. The oversight personnel must complete CDT's annual training, conduct an annual assessment of its covered AI systems, as specified, and submit a summary of the assessment findings to CDT.

FISCAL EFFECT:

1) Costs (General Fund (GF)) to CDT, likely in the low millions of dollars annually. CDT anticipates needing three permanent positions and $1.8 million in the first year of implementation and $1.5 million ongoing thereafter to implement a tracking management system, complete training certification and on-going reaccreditation, and complete training obligations.

2) Costs (GF, special funds) to each state agency that operates a covered AI system to develop a human oversight mechanism and fulfill the bill's assessment and reporting requirements. In the aggregate, these costs may be in the tens of millions of dollars annually, depending on how many agencies are affected and how much work it takes to achieve compliance for each covered AI system. As of when this analysis was prepared, the following state agencies reported fiscal impacts:

   - Office of Emergency Services (CalOES) anticipates costs (GF) of approximately $4.6 million in the first year of implementation and $2.6 million ongoing thereafter for six full-time positions in its Information Technology and Homeland Security Divisions. These costs cover salary, benefits, and private sector trainings for these positions to ensure they stay up-to-date with changes in AI technology, plus software and AI security monitoring tools.

   - Costs (GF) to California Department of Forestry and Fire Protection (CAL FIRE) of an unknown but potentially significant amount. CAL FIRE reports it already uses human oversight for AI tools but was unable to provide an estimate of its cost for doing so, or its expected costs for the bill's assessment and reporting requirements. These costs may be in the hundreds of thousands to millions of dollars, depending on actual staffing needs.

COMMENTS:

1) **Background.** As detailed in the analysis of this bill by the Assembly Committee on Privacy and Consumer Protection, many state agencies use AI technologies and ADS to help operate California's critical infrastructure. However, according to the author:

   > Currently, there is no standardized approach to human oversight of AI systems in critical infrastructure, creating inconsistent safety practices across vital sectors….Artificial Intelligence must remain a tool controlled by humans, not the other way around.

   AI technology is not a perfect tool: among other issues, it replicates biases and errors that are present in its training data and requires significant human review to ensure the accuracy and completeness of its work. The risks of unsupervised AI systems that help operate critical infrastructure are high because of the importance of this infrastructure to the functioning of the state. This bill imposes training and reporting requirements on state agencies that deploy covered AI systems that affect the state's critical infrastructure, and requires agencies to develop human oversight mechanisms to monitor applicable AI systems in real time as they operate.

2) **Related Legislation.** AB 979 (Irwin) requires CalOES's California Cybersecurity Integration Center to develop a playbook to facilitate information sharing across the AI community and to strengthen collective cyber defenses against emerging threats. AB 979 is pending in the Senate Appropriations Committee.

   AB 1018 (Bauer-Kahan) imposes reporting, appeal, and auditing requirements on developers and deployers of ADS used to make or facilitate a consequential decision, including state agencies that deploy covered ADS. AB 1018 is pending in the Senate Appropriations Committee.

SB 53 (Wiener), among other provisions, imposes reporting and auditing requirements on large developers of foundation AI models and enacts whistleblower protections related to risky activities of large developers. SB 53 is pending in this committee.

Analysis Prepared by: Annika Carlson / APPR. / (916) 319-2081