II

118TH CONGRESS
2D SESSION

S. 4956

To regulate electronic medical device use in secure compartmented information facilities, to require the Director of the National Intelligence oversee transparency reporting and related initiatives, to encourage investment in modernization efforts for sensitive compartmented information facilities, and for other purposes.

IN THE SENATE OF THE UNITED STATES

AUGUST 1, 2024

Mr. WELCH (for himself and Mr. CASEY) introduced the following bill; which was read twice and referred to the Select Committee on Intelligence

---

A BILL

To regulate electronic medical device use in secure compartmented information facilities, to require the Director of the National Intelligence oversee transparency reporting and related initiatives, to encourage investment in modernization efforts for sensitive compartmented information facilities, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cleared Locations Enabling Access to Relevant Essential Devices Act of 2024'' or the ''CLEARED Act of 2024''.

SEC. 2. ENHANCING NATIONAL ACCESSIBILITY FOR BETTER LONG-TERM EMPLOYMENT ACT OF 2024.

(a) DEFINITIONS.—In this section:

(1) COVERED ENTITY.—The term ''covered entity'' means any entity that—

(A) is established under or sponsored by any branch of the United States Government; and

(B) manages a secure compartmented information facility.

(2) ELECTRONIC MEDICAL DEVICE.—The term ''electronic medical device'' has the meaning given that term in Intelligence Community Directive 124.

(3) GOVERNANCE BOARD.—The term ''Governance Board'' means the Electronic Medical Device Governance Board described in Intelligence Community Directive 124.

(b) DEVICE APPROVAL DISCLOSURE.—

(1) ELECTRONIC MEDICAL DEVICE LEDGERS.—Beginning on the date of the enactment of this Act, the head of any covered entity shall begin developing and maintaining, for each secure compartmented information facility managed by such covered entity, a ledger to track the approval and denial of requests for electronic medical device use, which shall include—

(A) a case-by-case annotation of each approval or denial of an electronic medical device;

(B) a justification for each such approval or denial;

(C) any relevant details regarding device restrictions or accommodations; and

(D) statistics summarizing the number of electronic medical devices approved for unrestricted use and limited use and devices that were denied.

(2) APPROVED ELECTRONIC MEDICAL DEVICE LIST.—

(A) IN GENERAL.—Beginning not later than 1 year after the date of the enactment of this Act, the head of any covered entity shall develop and maintain, for each secure compartmented information facility managed by such covered entity, develop and maintain a list that includes the following:

(i) Each electronic medical device that is approved for unrestricted use in the facility.

(ii) Each electronic medical device that is approved for limited use in the facility, including—

(I) any restrictions or accommodations required with respect to each such device;

(II) a description of whether such restrictions or accommodations vary from restrictions imposed or accommodations provided by other covered entities; and

(III) if applicable, an explanation of the variability of such restrictions or accommodations.

(iii) Each electronic medical device that is denied for use in the facility and the justification for such denial.

(B) FORM.—

(i) ACCESS TO UNCLASSIFIED LIST.—The relevant list of a covered entity developed pursuant to subparagraph (A) shall be—

(I) unclassified to the maximum extent practicable, but may include a classified annex; and

(II) provided to any applicant or employee of the covered entity who seeks a position that requires access

to a secure compartmented information facility.

(ii) ACCESS TO CLASSIFIED LIST.—

(I) CLEARED APPLICANTS.—On the date that an applicant or employee described in clause (i)(II) receives the security clearance necessary for access to the secure compartmented information facility, the head of the relevant covered entity shall make available to such applicant or employee the classified portion of the list described in clause (i).

(II) EXISTING EMPLOYEES.—Not later than 1 year after the date of the enactment of this Act, the head of each covered entity shall provide to each employee of the covered entity who has the security clearance necessary to access a secure compartmented information facility, the list developed by the head of such covered entity with respect to such facility, which shall be unclassified to the max-

imum extent practicable, but may include a classified annex.

(3) ELECTRONIC MEDICAL DEVICE POLICY.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the head of each covered entity shall develop a policy for the use of electronic medical devices in secure compartmented information facilities, which shall include a list of the types of electronic medical devices that are approved for use in each such facility managed by the covered entity.

(B) ANNUAL REVIEW.—The head of each covered entity shall annually review any policy developed pursuant to subparagraph (A).

(4) SUBMISSION TO DIRECTOR OF NATIONAL INTELLIGENCE AND GOVERNANCE BOARD.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter, the head of each covered entity shall submit to the Director of National Intelligence and the Governance Board—

(A) any ledger developed pursuant to paragraph (1);

(B) any list published pursuant to paragraph (2)(A); and

(C) any policy developed pursuant to paragraph (3)(A).

(c) REVIEW OF ELECTRONIC MEDICAL DEVICE SECURITY.—

(1) IN GENERAL.—The Governance Board shall review electronic medical device security and equity concerns for covered agencies.

(2) DUTIES.—The Governance Board shall—

(A) review the policies of covered agencies regarding the use of electronic medical devices in secure compartmented information facilities;

(B) review each ledger or list submitted in accordance with subsection (b)(4);

(C) identify and resolve discrepancies in such ledgers and lists, with respect to both variation in justifications for restrictions and accommodations and denials within each covered entity and across all covered entities;

(D) facilitate and direct security research and technical risk assessments on electronic medical devices and determine threats to national security posed by such devices;

(E) for electronic medical devices that have been researched pursuant to subparagraph (D),

evaluate threat mitigation measures available and the efficacy ratings of such measures; and

(F) provide recommendations for risk management of electronic medical devices in secure compartmented information facilities.

(3) ELECTRONIC MEDICAL LEDGER DATABASE.—

(A) IN GENERAL.—Using each ledger and list submitted to the Governance Board in accordance with subsection (b)(4), the Governance Board shall develop and maintain a publicly accessible database of electronic medical devices that have been approved or denied for use at any secure compartmented information facility, including, to the extent practicable—

(i) approval rates;

(ii) accommodations or restrictions for usage; and

(iii) for each covered entity, specific processes for electronic medical device approval.

(B) PUBLIC AVAILABILITY OF INFORMATION.—The Governance Board shall make available on the website of the Office of the Director of National Intelligence the following:

(i) General approval and denial rates for devices described in subparagraph (A) of different types.

(ii) Points of contact for teams responsible for approvals and denials of devices described in subparagraph (A).

(C) LEDGER DISCREPANCIES.—The Governance Board shall include in such database any discrepancy identified pursuant to paragraph (2), including, for each such discrepancy—

(i) a detailed description of the discrepancy; and

(ii) proposed remediations.

(D) FORM.—The database shall be unclassified, but may include a classified annex as the Director of National Intelligence considers appropriate.

(4) REPORT.—

(A) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, and annually thereafter, the Governance Board shall submit to the Director of National Intelligence a report on the state of electronic medical de-

vice usage in secure compartmented information facilities.

(B) CONTENT.—Each report submitted pursuant to subparagraph (A) shall include—

(i) a description of the research efforts, risk management recommendations, and strategic approaches of the Governance Board to support changes or innovations that improve the use of electronic medical devices in secure compartmented information facilities;

(ii) a description of any barriers to resolving discrepancies under paragraph (2)(C);

(iii) a summary of statistics describing approval rates gleaned from the database developed pursuant to paragraph (3); and

(iv) any other information the Governance Board determines is relevant for the Director of National Intelligence to consider regarding the use of electronic medical devices in secure compartmented information facilities.

(5) ANNUAL EVALUATIONS.—Not later than 180 days after receiving a report under paragraph (4), the Director of National Intelligence shall—

(A) evaluate the findings and recommendations of the Governance Board in such report; and

(B) submit to Congress a report that includes—

(i) the results of the evaluation conducted under subparagraph (A);

(ii) a description of current approval rates for electronic medical devices;

(iii) a description of research efforts and risk mitigation strategies with respect to electronic medical devices; and

(iv) recommendations for updating electronic medical device requirements in secure compartmented information facilities.

(d) PROTECTION OF INFORMATION.—In carrying out this section, the head of each covered entity shall ensure the protection of personally identifiable information, including medical information, in accordance with all appli-

cable laws and policies with respect to confidentiality and privacy.

○