

119TH CONGRESS
2D SESSION

H. R. 10189

To amend title 10, United States Code, to direct the Secretary of Defense to establish an artificial intelligence incident and vulnerability reporting program, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

AUGUST 31, 2026

Ms. JACOBS (for herself, Mr. MORAN, and Mr. WHITESIDES) introduced the following bill; which was referred to the Committee on Armed Services

A BILL

To amend title 10, United States Code, to direct the Secretary of Defense to establish an artificial intelligence incident and vulnerability reporting program, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Defense AI Reliability
5 and Reporting Act”.

1 **SEC. 2. DEPARTMENT OF DEFENSE AI INCIDENT AND VUL-**
2 **NERABILITY REPORTING PROGRAM.**

3 Chapter 131 of title 10, United States Code, is
4 amended by inserting after section 2224a the following
5 new section:

6 **“§ 2224b. Artificial intelligence incident and vulner-**
7 **ability reporting program**

8 “(a) IN GENERAL.—The Secretary of Defense shall
9 establish a centralized Department-wide program for the
10 reporting, tracking, analysis, and remediation of covered
11 AI incidents and covered AI vulnerabilities arising from
12 the development, testing, procurement, fielding, or oper-
13 ation of artificial intelligence systems within the Depart-
14 ment of Defense.

15 “(b) PURPOSE.—The purpose of the program estab-
16 lished under subsection (a) shall be to—

17 “(1) identify recurring risks, failure modes,
18 vulnerabilities, and systemic weaknesses in artificial
19 intelligence systems, including risks or failure modes
20 arising from human-machine teaming;

21 “(2) support mitigation of significant risks; and

22 “(3) inform testing, procurement, cybersecurity,
23 and deployment decisions to improve the safety, se-
24 curity, reliability, and operational effectiveness of
25 such systems.

1 “(c) REQUIREMENTS FOR PROGRAM.—The program
2 shall—

3 “(1) be designed using practices drawn from es-
4 tablished safety incident reporting programs, vulner-
5 ability disclosure programs, and programs to identify
6 and develop lessons learned;

7 “(2) emphasize non-punitive reporting, protec-
8 tion of sensitive and proprietary information, and
9 dissemination of lessons learned, as appropriate; and

10 “(3) include a mechanism to enable timely ac-
11 cess to and sharing of relevant logs, system data,
12 and model information as necessary to support anal-
13 ysis and response.

14 “(d) DESIGNATION OF OFFICIAL.—The Secretary
15 shall designate an appropriate official for the reporting,
16 tracking, analysis, and remediation of covered AI incidents
17 and covered AI vulnerabilities under this section. The Sec-
18 retary, acting through such official, shall receive and
19 standardize reports, conduct trend analysis, identify recur-
20 ring risks and failure modes, and issue guidance, alerts,
21 and recommendations, as appropriate.

22 “(e) REPORTING AND CATEGORIZATION.—(1) The
23 Secretary shall require prompt reporting to the official
24 designated under subsection (d) of—

25 “(A) any covered AI incident; and

1 “(B) any covered AI vulnerability.

2 “(2) The Secretary, acting through the official, shall
3 categorize each incident or vulnerability reported to the
4 official according to whether the incident or vulnerability
5 requires—

6 “(A) a Department-wide response;

7 “(B) a response at the program level; or

8 “(C) a response at a local level.

9 “(f) DEPARTMENT-WIDE AND PROGRAM-LEVEL
10 MATTERS.—(1) In the case of any incident or vulner-
11 ability categorized under subsection (e)(2)(A) or (B), the
12 Secretary, acting through the official designated under
13 subsection (d), shall coordinate any responses that the
14 Secretary considers appropriate, such as remediation, re-
15 testing, mitigation measures, or deployment restrictions.

16 “(2) In addition, in the case of any incident or vulner-
17 ability described in subsection (e)(2)(A), the Secretary,
18 acting through the official, shall require—

19 “(A) a documented corrective action plan; and

20 “(B) validation that the mitigation measures, if
21 any, in such plan have been implemented before con-
22 tinued operational use.

23 “(g) PROTECTION OF REPORTS.—(1) The Secretary
24 shall establish a protected disclosure process, informed by
25 established vulnerability disclosure practices, through

1 which members of the Armed Forces, civilian employees,
2 contractors, and subcontractors at any tier may report
3 covered AI incidents and covered AI vulnerabilities in good
4 faith.

5 “(2) The Secretary shall ensure that a person making
6 a report in good faith under paragraph (1) is not, on the
7 basis of that report alone, subject to adverse contract ac-
8 tion, subject to adverse personnel action, or otherwise re-
9 taliated against by the Department.

10 “(h) PROTECTION OF INFORMATION.—The Secretary
11 shall establish procedures to protect sensitive, proprietary,
12 and classified information submitted through the pro-
13 tected disclosure process under subsection (g).

14 “(i) ANNUAL REPORT.—(1) In each of years 2027
15 through 2031, the Secretary shall submit to the congres-
16 sional defense committees an annual report on the pro-
17 gram. The report shall include—

18 “(A) the number of reports made of incidents
19 and vulnerabilities and the categorizations of such
20 reports;

21 “(B) a summary of significant trends, recurring
22 risks, systemic issues, and corrective actions taken
23 in response;

24 “(C) in the case of any covered AI incident re-
25 sulting in the loss of life of, or in bodily harm to,

1 a member of the Army, Navy, Marine Corps, Air
2 Force, or Space Force—

3 “(i) a description of the incident, including
4 the system or systems involved and the oper-
5 ational context;

6 “(ii) the date and time the incident oc-
7 curred;

8 “(iii) an assessment of the cause and oper-
9 ational consequence of the incident; and

10 “(iv) any corrective actions taken; and

11 “(D) any recommendations for changes to test-
12 ing, procurement, cybersecurity, or deployment poli-
13 cies relating to artificial intelligence systems.

14 “(2) Each report under this subsection shall be sub-
15 mitted in unclassified form but may include a classified
16 annex.

17 “(j) DEFINITIONS.—In this section:

18 “(1) The term ‘artificial intelligence’ has the
19 meaning given such term in section 5002 of the Na-
20 tional Artificial Intelligence Initiative Act of 2020
21 (15 U.S.C. 9401).

22 “(2) The term ‘covered AI incident’ means an
23 event in which an artificial intelligence system—

24 “(A) causes unintended operational, safety,
25 or security harm;

1 “(B) operates outside authorized param-
2 eters or approved safety, legal, or mission
3 guardrails;

4 “(C) materially degrades mission perform-
5 ance or reliability in a real-world or operation-
6 ally representative environment;

7 “(D) fails to respond to an operator dis-
8 engage command;

9 “(E) operates in a manner that, under rea-
10 sonably foreseeable circumstances, could have
11 resulted in significant unintended operational,
12 safety, or security harm; or

13 “(F) operates in a manner that raises con-
14 cerns regarding system control and autonomy.

15 “(3) The term ‘covered AI vulnerability’ means
16 an exploitable weakness, vulnerability, or systemic
17 issue in an artificial intelligence system or related
18 component that could materially affect mission per-
19 formance, compromise system integrity, create safety
20 risk, or result in unauthorized or unintended behav-
21 ior.”.

○