

119TH CONGRESS
2D SESSION

H. R. 8710

To amend title 10, United States Code, to require the Secretary of Defense to implement resilient capabilities to recover critical Department of Defense data in the event such data is lost, degraded, or destroyed, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MAY 7, 2026

Mr. SUBRAMANYAM (for himself and Mr. McCORMICK) introduced the following bill; which was referred to the Committee on Armed Services

A BILL

To amend title 10, United States Code, to require the Secretary of Defense to implement resilient capabilities to recover critical Department of Defense data in the event such data is lost, degraded, or destroyed, 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 “National Defense Data
5 Resilience Act”.

1 **SEC. 2. DATA RECOVERY REQUIREMENTS AND STRATEGY.**

2 (a) DATA RECOVERY REQUIREMENTS.—Chapter 19
3 of title 10, United States Code, is amended by inserting
4 after section 391b the following new section:

5 **“§ 391c. Data recovery requirements**

6 “(a) MANDATORY RECOVERY TIME OBJECTIVES.—

7 “(1) The Secretary of Defense shall, with re-
8 spect to each element of the Department of Defense,
9 carry out the following:

10 “(A) Designate data as one of the fol-
11 lowing types, as applicable:

12 “(i) Critical data.

13 “(ii) Important data.

14 “(iii) Necessary data.

15 “(B) Not later than 180 days after the
16 date of the enactment of this section, establish
17 mandatory recovery time objectives for data so
18 designated as critical data.

19 “(C) Not later than 270 days after the
20 date of the enactment of this section, establish
21 mandatory recovery time objectives for data so
22 designated as important data or necessary data.

23 “(2) Each recovery time objective established
24 under paragraph (1) shall satisfy the following re-
25 quirements:

1 “(A) Be based upon the type of data to
2 which such objective applies, including with re-
3 spect to threat exposure.

4 “(B) Be updated in response to intel-
5 ligence on evolving threats from state and non-
6 state actors, including the People’s Republic of
7 China.

8 “(3) Not later than one year after the date of
9 the enactment of this section and annually there-
10 after, the Secretary of Defense shall, for each ele-
11 ment of the Department of Defense, submit to the
12 congressional defense committees an auditable recov-
13 ery certification report that includes information re-
14 lating to the following:

15 “(A) Each recovery time objective that is
16 established under paragraph (1) and applies to
17 such element.

18 “(B) Whether such objective satisfies the
19 requirements listed in paragraph (2).

20 “(b) DATA RECOVERY CAPABILITY REQUIRE-
21 MENTS.—

22 “(1) Not later than 180 days after the date of
23 the enactment of this section, the Secretary of De-
24 fense shall, for data designated as critical data pur-
25 suant to subparagraph (A) of subsection (a)(1), field

1 data recovery capabilities that satisfy the following
2 requirements:

3 “(A) Prioritize providing critical services in
4 support of national defense.

5 “(B) Include the following:

6 “(i) Immutable backups that satisfy
7 the following requirements:

8 “(I) Preserve logically separated
9 copies of data.

10 “(II) Are selectively segmented
11 or isolated from external networks by
12 means of software, firewalls, or other
13 controls.

14 “(ii) Continuous monitoring of backup
15 environments to detect tampering, insider
16 threats, and malicious corruption.

17 “(iii) Annual recovery exercises that
18 simulate sophisticated nation-state
19 cyberattacks designed to cripple data sys-
20 tems.

21 “(iv) Audits in which external or in-
22 ternal independent groups mimic tactics,
23 techniques, and procedures of cyberattacks
24 to assess and validate the ability of each
25 element of the Department of Defense to

1 carry out the objectives established under
2 such subsection with respect to realistic
3 threat conditions.

4 “(2) Not later than 270 days after the date of
5 the enactment of this section, the Secretary of De-
6 fense shall, for data designated as important data or
7 necessary data pursuant to subsection (a)(1)(A),
8 field data recovery capabilities described in para-
9 graph (1).

10 “(c) APPROVED TECHNOLOGY STANDARDS.—In
11 fielding a data recovery capability under subsection (b),
12 the Secretary of Defense may not adopt technology unless
13 the following requirements are satisfied:

14 “(1) Such technology is listed in an inventory
15 of the Department of Defense for certified cyberse-
16 curity and data protection technology.

17 “(2) If such technology is technology for recov-
18 ering or repairing damaged or lost data, such tech-
19 nology provides for the following:

20 “(A) Immutable storage.

21 “(B) Robust recovery capabilities.

22 “(C) Full audit trails.

23 “(D) Continuous monitoring for data in-
24 tegrity and anomalous activity.

25 “(d) DEFINITIONS.—In this section:

1 “(1) The term ‘critical data’ means data, so
2 vital to the United States, that the incapacity or de-
3 struction of such data would have a debilitating im-
4 pact on security, national economic security, national
5 public health or safety, or any combination thereof.

6 “(2) The term ‘data recovery capability’ means
7 a technology, process, or governance framework to
8 ensure rapid, secure, and verifiable recovery after a
9 destructive cyberattack.

10 “(3) The term ‘important data’ means data
11 that is important to the United States and the inca-
12 pacity or destruction of such data would have a sig-
13 nificant impact on security, national economic secu-
14 rity, national public health or safety, or any com-
15 bination thereof.

16 “(4) The term ‘necessary data’ means data, the
17 incapacity or destruction of which would have a
18 measurable impact on security, national economic se-
19 curity, national public health or safety, or any com-
20 bination thereof.

21 “(5) The term ‘recovery time objective’ means
22 the maximum allowable time the Secretary of De-
23 fense determines necessary to restore critical func-
24 tions and data following a cyberattack.”.

1 (b) CLERICAL AMENDMENT.—The table of sections
2 for chapter 19 of title 10, United States Code, is amended
3 by inserting after the item relating to section 391b the
4 following new item:

“391c. Data recovery requirements.”.

5 (c) DATA RECOVERY STRATEGY.—

6 (1) Not later than 90 days after the date of the
7 enactment of this Act, the Secretary of Defense shall
8 submit to the congressional defense committees a
9 data recovery strategy for the Department of De-
10 fense that includes information relating to the fol-
11 lowing:

12 (A) Recovery time objectives for such
13 strategy.

14 (B) The technology necessary for such ob-
15 jectives.

16 (C) Oversight processes with respect to
17 such strategy.

18 (D) The funds necessary to carry out such
19 strategy.

20 (2) The strategy under paragraph (1) shall be
21 submitted in unclassified form, but may contain a
22 classified annex.

23 (3) In this subsection, the term “recovery time
24 objective” means the maximum allowable time the

- 1 Secretary of Defense determines necessary to restore
- 2 critical functions and data following a cyberattack.

○