

119TH CONGRESS
1ST SESSION

S. 3161

To enhance protection of data affecting operational security of Department of Defense personnel, and for other purposes.

IN THE SENATE OF THE UNITED STATES

NOVEMBER 7, 2025

Ms. SLOTKIN (for herself and Ms. ERNST) introduced the following bill; which was read twice and referred to the Committee on Armed Services

A BILL

To enhance protection of data affecting operational security of Department of Defense personnel, 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 “Protecting DOD Data
5 Act of 2025”.

6 **SEC. 2. ENHANCED PROTECTION OF DATA AFFECTING**
7 **OPERATIONAL SECURITY OF DEPARTMENT**
8 **OF DEFENSE PERSONNEL.**

9 (a) **PRIORITIES FOR PROTECTION OF PERSONAL**
10 **DATA FOR OPERATIONAL SECURITY.**—In carrying out the

1 duties of the Secretary of Defense, the Secretary shall
2 identify and prioritize the protection of personal data that
3 is related to or may have impacts on the operational secu-
4 rity of members of the Armed Forces and civilian employ-
5 ees of the Department of Defense through the prevention
6 of collection, use, dissemination, or retention of such data
7 that does not conform with provisions of law and practices
8 relating to privacy that were in effect on the day before
9 the date of the enactment of this Act.

10 (b) REVIEW AND ISSUANCE OF NEW GUIDANCE RE-
11 LATED TO PROTECTION OF PERSONAL DATA RELATED TO
12 OPERATIONAL SECURITY.—Not later than June 1, 2026,
13 the Secretary of Defense shall review all applicable guid-
14 ance and policy relating to the protection of personal data
15 that is related to or may have impacts on the operational
16 security of Department personnel and, if necessary, issue
17 revised or new guidance for enhanced protection measures
18 for such data. Such guidance shall cover provisions of law
19 and practices relating to privacy and personnel security
20 that were in effect on the day before the date of the enact-
21 ment of this Act.

22 (c) STORAGE OF DATA.—

23 (1) LIMITATION.—The Secretary shall ensure
24 that no Department personal data related to or that
25 may have impacts on the operational security of De-

1 partment personnel is stored on a non-Department
2 server or cloud service except pursuant to a contract
3 or other agreement entered into by the Secretary
4 and a contractor or subcontractor of the Department
5 or, for personnel data, with the permission of the
6 data subject.

7 (2) WAIVERS.—The Secretary may waive para-
8 graph (1) in a case in which the Secretary certifies
9 in writing that such waiver—

10 (A) appropriately considers the operational
11 security risks to an employee of the Department
12 with respect to whom such data may relate;

13 (B) does not pose a risk to national secu-
14 rity; and

15 (C) is necessary in the interest of national
16 security.

17 (d) CONGRESSIONAL NOTIFICATION OF CHANGES TO
18 DEPARTMENTAL ISSUANCES.—

19 (1) IN GENERAL.—Not later than 30 days after
20 the date on which the Secretary changes a Depart-
21 ment issuance relating to the protection of personal
22 data that is related to or may have impacts on the
23 operational security of Department personnel, the
24 Secretary shall submit to Congress notice of the
25 change.

1 (2) SUNSET.—The requirement of paragraph
2 (1) shall terminate on the date that is five years
3 after the date of the enactment of this Act.

4 (e) CONGRESSIONAL NOTIFICATION OF EVENTS.—

5 (1) IN GENERAL.—Not later than 30 days after
6 the date of the occurrence of an event described in
7 paragraph (2), the Secretary shall submit to Con-
8 gress notice of the event.

9 (2) EVENTS DESCRIBED.—An event described
10 in this paragraph is an occurrence of an event in
11 which—

12 (A) the Secretary issues a waiver under
13 subsection (c)(2);

14 (B) personal data related to or that may
15 have an impact on operational security of De-
16 partment personnel is not stored according to
17 Department regulations or exfiltrated in viola-
18 tion of Department regulations;

19 (C) personal data related to or that may
20 have an impact on operational security of De-
21 partment personnel is stored on a non-Depart-
22 ment server or cloud service that has not under-
23 gone an authorization process in accordance
24 with Department regulations; or

1 (D) personal data related to or that may
2 have an impact on operational security of De-
3 partment of Defense personnel is exposed in
4 any cybersecurity incident.

5 (f) STANDARDS, TRAINING, AND REPORTING PROC-
6 ESSES FOR SYSTEM OWNERS.—

7 (1) IN GENERAL.—The Secretary shall develop
8 standards, training, reporting, and security debrief-
9 ing requirements for Department personnel who re-
10 ceive write or read access privileges as system own-
11 ers across more than one platform of Department
12 information systems that hosts personal data related
13 to or that may have an impact on operational secu-
14 rity of Department personnel.

15 (2) SECURITY DEBRIEFINGS.—The Secretary
16 shall ensure that personnel described in paragraph
17 (1) are provided regular security debriefings, includ-
18 ing after departing the Department.

19 (3) NOTIFICATION OF CONGRESS UNDER CER-
20 TAIN CIRCUMSTANCES.—Not later than 30 days
21 after the completion of the development of the
22 standards, training, reporting, and security debrief-
23 ing requirements in paragraph (1) the Secretary
24 shall submit to Congress details of the requirements.

○