

118TH CONGRESS  
1ST SESSION

**S.** \_\_\_\_\_

To require reporting of suspicious transmissions in order to assist in criminal investigations and counterintelligence activities relating to international terrorism, and for other purposes.

---

IN THE SENATE OF THE UNITED STATES

Mr. MANCHIN (for himself and Mr. CORNYN) introduced the following bill;  
which was read twice and referred to the Committee on

---

**A BILL**

To require reporting of suspicious transmissions in order to assist in criminal investigations and counterintelligence activities relating to international terrorism, 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 “See Something, Say  
5 Something Online Act of 2023”.

6 **SEC. 2. SENSE OF CONGRESS.**

7 It is the sense of Congress that—

1           (1) section 230 of the Communications Act of  
2           1934 (47 U.S.C. 230) (commonly known as the  
3           “Communications Decency Act of 1996”) was never  
4           intended to provide legal protection for websites or  
5           interactive computer service providers that do noth-  
6           ing after becoming aware of instances of individuals  
7           or groups planning, committing, promoting, and fa-  
8           cilitating terrorism, serious drug offenses, and vio-  
9           lent crimes;

10           (2) it is not the intent of this Act to remove or  
11           strip all liability protection from websites or inter-  
12           active computer service providers that are  
13           proactively working to resolve these issues; and

14           (3) should websites or interactive computer  
15           service providers fail to exercise due care in the im-  
16           plementation, filing of the suspicious transmission  
17           activity reports, and reporting of major crimes, Con-  
18           gress intends to look at removing liability protections  
19           under the Communications Decency Act of 1996 in  
20           its entirety.

21 **SEC. 3. DEFINITIONS.**

22           In this Act:

23           (1) DEPARTMENT.—The term “Department”  
24           means the Department of Justice.

1           (2) INTERACTIVE COMPUTER SERVICE.—The  
2 term “interactive computer service” has the meaning  
3 given the term in section 230 of the Communica-  
4 tions Act of 1934 (47 U.S.C. 230).

5           (3) KNOWN SUSPICIOUS TRANSMISSION.—The  
6 term “known suspicious transmission” means any  
7 suspicious transmission that a provider of an inter-  
8 active computer service—

9                   (A) should have reasonably known to have  
10 occurred; or

11                   (B) was notified of by a director, officer,  
12 employee, agent, interactive computer service  
13 user, or State or Federal law enforcement agen-  
14 cy.

15           (4) MAJOR CRIME.—The term “major crime”  
16 means a Federal criminal offense—

17                   (A) that is a crime of violence (as defined  
18 in section 16 of title 18, United States Code);

19                   (B) relating to domestic or international  
20 terrorism (as those terms are defined in section  
21 2331 of title 18, United States Code); or

22                   (C) that is a serious drug offense (as de-  
23 fined in section 924(e) of title 18, United  
24 States Code).

1           (5) STAR.—The term “STAR” means a sus-  
2           picious transmission activity report required to be  
3           submitted under section 3.

4           (6) SUSPICIOUS TRANSMISSION.—The term  
5           “suspicious transmission” means any public or pri-  
6           vate post, message, comment, tag, transaction, or  
7           any other user-generated content or transmission  
8           that commits, facilitates, incites, promotes, or other-  
9           wise assists the commission of a major crime.

10 **SEC. 4. REPORTING OF SUSPICIOUS ACTIVITY.**

11           (a) MANDATORY REPORTING OF SUSPICIOUS TRANS-  
12           MISSIONS.—

13           (1) IN GENERAL.—If a provider of an inter-  
14           active computer service detects a suspicious trans-  
15           mission, the provider, including any director, officer,  
16           employee, agent, or representative of the provider,  
17           shall submit to the Department a STAR describing  
18           the suspicious transmission in accordance with this  
19           section.

20           (2) REQUIREMENTS.—

21           (A) IN GENERAL.—Except as provided in  
22           subparagraph (C), a STAR required to be sub-  
23           mitted under paragraph (1) shall be submitted  
24           not later than 30 days after the date on which

1 the provider of an interactive computer serv-  
2 ice—

3 (i) initially detects the suspicious  
4 transmission; or

5 (ii) is alerted to the suspicious trans-  
6 mission on the platform of such service.

7 (B) IMMEDIATE NOTIFICATION.—In the  
8 case of a suspicious transmission that requires  
9 immediate attention, such as an active sale or  
10 solicitation of sale of drugs or a threat of ter-  
11 rorist activity, the provider of an interactive  
12 computer service shall—

13 (i) immediately notify, by telephone,  
14 an appropriate law enforcement authority;  
15 and

16 (ii) file a STAR in accordance with  
17 this section.

18 (C) DELAY OF SUBMISSION.—The 30-day  
19 period described in subparagraph (A) may be  
20 extended by 30 days if the provider of an inter-  
21 active computer service provides a valid reason  
22 to the agency designated or established under  
23 subsection (b)(2).

24 (b) REPORTING PROCESS.—

1           (1) IN GENERAL.—The Attorney General shall  
2           establish a process by which a provider of an inter-  
3           active computer service may submit STARS under  
4           this section.

5           (2) DESIGNATED AGENCY.—

6           (A) IN GENERAL.—In carrying out this  
7           section, the Attorney General shall designate an  
8           agency within the Department, or, if the Attor-  
9           ney General determines appropriate, establish a  
10          new agency within the Department, to which  
11          STARS should be submitted under subsection  
12          (a).

13          (B) CONSUMER REPORTING.—The agency  
14          designated or established under subparagraph  
15          (A) shall establish a centralized online resource,  
16          which may be used by individual members of  
17          the public to report suspicious activity related  
18          to major crimes for investigation by the appro-  
19          priate law enforcement or regulatory agency.

20          (C) COOPERATION WITH INDUSTRY.—The  
21          agency designated or established under sub-  
22          paragraph (A)—

23                  (i) may conduct training for enforce-  
24                  ment agencies and for providers of inter-

1 active computer services on how to cooper-  
2 ate in reporting suspicious activity;

3 (ii) may develop relationships for pro-  
4 motion of reporting mechanisms and re-  
5 sources available on the centralized online  
6 resource required to be established under  
7 subparagraph (B); and

8 (iii) shall coordinate with the National  
9 White Collar Crime Center to convene ex-  
10 perts to design training programs for State  
11 and local law enforcement agencies, which  
12 may include using social media, online ads,  
13 paid placements, and partnering with ex-  
14 pert non-profit organizations to promote  
15 awareness and engage with the public.

16 (c) CONTENTS.—Each STAR submitted under this  
17 section shall contain, at a minimum—

18 (1) the name, location, and other such identi-  
19 fication information as submitted by the user to the  
20 provider of the interactive computer service;

21 (2) the date and nature of the post, message,  
22 comment, tag, transaction, or other user-generated  
23 content or transmission detected for suspicious activ-  
24 ity such as time, origin, and destination; and

1           (3) any relevant text, information, and  
2 metadata related to the suspicious transmission.

3           (d) RETENTION OF RECORDS AND NONDISCLO-  
4 SURE.—

5           (1) RETENTION OF RECORDS.—Each provider  
6 of an interactive computer service shall—

7                   (A) maintain a copy of any STAR sub-  
8 mitted under this section and the original  
9 record equivalent of any supporting documenta-  
10 tion for the 5-year period beginning on the date  
11 on which the STAR was submitted;

12                   (B) make all supporting documentation  
13 available to the Department and any appro-  
14 priate law enforcement agencies upon request;  
15 and

16                   (C) not later than 30 days after the date  
17 on which the provider submits a STAR under  
18 this section, take action against the website or  
19 account reported unless the provider receives a  
20 notification from a law enforcement agency that  
21 the website or account should remain open.

22           (2) NONDISCLOSURE.—Except as otherwise  
23 prescribed by the Attorney General, no provider of  
24 an interactive computer service, or officer, director,  
25 employee, or agent of such a provider, subject to an

1 order under subsection (a) may disclose the exist-  
2 ence of, or terms of, the order to any person.

3 (e) DISCLOSURE TO OTHER AGENCIES.—

4 (1) IN GENERAL.—Subject to paragraph (2),  
5 the Attorney General shall—

6 (A) ensure that STARS submitted under  
7 this section and reports from the public sub-  
8 mitted under subsection (b)(2)(B) are referred  
9 as necessary to the appropriate Federal, State,  
10 or local law enforcement or regulatory agency;

11 (B) make information in a STAR sub-  
12 mitted under this section available to an agen-  
13 cy, including any State financial institutions su-  
14 pervisory agency or United States intelligence  
15 agency, upon request of the head of the agency;  
16 and

17 (C) develop a strategy to disseminate rel-  
18 evant information in a STAR submitted under  
19 this section in a timely manner to other law en-  
20 forcement and government agencies, as appro-  
21 priate, and coordinate with relevant nongovern-  
22 mental entities, such as the National Center for  
23 Missing and Exploited Children.

1           (2) LIMITATION.—The Attorney General may  
2           only make a STAR available under paragraph (1)  
3           for law enforcement purposes.

4           (f) COMPLIANCE.—Any provider of an interactive  
5           computer service that fails to report a known suspicious  
6           transmission shall not be immune from civil or criminal  
7           liability for such transmission under section 230(c) of the  
8           Communications Act of 1934 (47 U.S.C. 230(c)).

9           (g) APPLICATION OF FOIA.—Any STAR submitted  
10          under this section, and any information therein or record  
11          thereof, shall be exempt from disclosure under section 552  
12          of title 5, United States Code, or any similar State, local,  
13          Tribal, or territorial law.

14          (h) RULEMAKING AUTHORITY.—Not later than 180  
15          days after the date of enactment of this Act, the Attorney  
16          General shall promulgate regulations to carry out this sec-  
17          tion.

18          (i) REPORT.—Not later than 180 days after the date  
19          of enactment of this Act, the Attorney General shall sub-  
20          mit to Congress a report describing the plan of the De-  
21          partment for implementation of this Act, including a  
22          breakdown of the costs associated with implementation.

23          (j) AUTHORIZATION OF APPROPRIATIONS.—There  
24          are authorized to be appropriated to the Attorney General  
25          such sums as may be necessary to carry out this Act.

1 **SEC. 5. AMENDMENT TO COMMUNICATIONS DECENCY ACT.**

2 Section 230(e) of the Communications Act of 1934  
3 (47 U.S.C. 230(e)) is amended by adding at the end the  
4 following:

5 “(6) LOSS OF LIABILITY PROTECTION FOR  
6 FAILURE TO SUBMIT SUSPICIOUS TRANSMISSION AC-  
7 TIVITY REPORT.—

8 “(A) DEFINITIONS.—In this paragraph,  
9 the terms ‘known suspicious transmission’ and  
10 ‘suspicious transmission’ have the meanings  
11 given those terms in section 3 of the See Some-  
12 thing, Say Something Online Act of 2023.

13 “(B) REQUIREMENT.—Any provider of an  
14 interactive computer service shall take reason-  
15 able steps to prevent or address unlawful users  
16 of the service through the reporting of sus-  
17 picious transmissions.

18 “(C) FAILURE TO COMPLY.—Any provider  
19 of an interactive computer service that fails to  
20 report a known suspicious transmission may be  
21 held liable as a publisher for the related sus-  
22 picious transmission.

23 “(D) RULE OF CONSTRUCTION.—Nothing  
24 in this paragraph shall be construed to impair  
25 or limit any claim or cause of action arising  
26 from the failure of a provider of an interactive

1 computer service to report a suspicious trans-  
2 mission.”.