

.....  
(Original Signature of Member)

118TH CONGRESS  
2D SESSION

**H. R.** \_\_\_\_\_

To establish an interagency working group to assess the challenges of protecting military and commercial telecommunications networks in the United States from security threats related to the Signaling System 7 telecommunication protocol standard, and for other purposes.

---

IN THE HOUSE OF REPRESENTATIVES

Mr. WEBER of Texas introduced the following bill; which was referred to the Committee on \_\_\_\_\_

---

**A BILL**

To establish an interagency working group to assess the challenges of protecting military and commercial telecommunications networks in the United States from security threats related to the Signaling System 7 telecommunication protocol standard, 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 “Securing Every Vector,  
5 Enhancing Networks Act” or the “SEVEN Act”.

1 **SEC. 2. SS7 INTERAGENCY WORKING GROUP AND REPORT**  
2 **ON ENSURING THE SECURITY AND INTEG-**  
3 **RITY OF TELECOMMUNICATIONS NETWORKS.**

4 (a) SS7 INTERAGENCY WORKING GROUP.—

5 (1) IN GENERAL.—Not later than 60 days after  
6 the date of the enactment of this Act, the Assistant  
7 Secretary of Commerce for Communications and In-  
8 formation, in consultation with the Director of the  
9 Cybersecurity and Infrastructure Security Agency,  
10 shall convene an interagency working group (in this  
11 section referred to as the “working group”) to pre-  
12 pare the annual reports under subsection (b) and  
13 provide the briefings under subsection (c).

14 (2) MEMBERSHIP.—

15 (A) IN GENERAL.—The working group  
16 shall consist of the following members:

17 (i) The Assistant Secretary of Com-  
18 merce for Communications and Informa-  
19 tion (or the designee of the Assistant Sec-  
20 retary), who shall serve as the Chair of the  
21 working group.

22 (ii) The Director of the Cybersecurity  
23 and Infrastructure Security Agency (or the  
24 designee of the Director), who shall serve  
25 as the Vice Chair of the working group.

1 (iii) Each of the following (or their  
2 designee):

3 (I) The Secretary of Homeland  
4 Security.

5 (II) The Director of the National  
6 Institute of Standards and Tech-  
7 nology.

8 (III) The Chief of Space Oper-  
9 ations.

10 (IV) The Attorney General.

11 (V) The Secretary of Defense.

12 (VI) The Chair of the Federal  
13 Communications Commission.

14 (VII) The head of any other com-  
15 ponent of the United States Govern-  
16 ment, regardless of whether such com-  
17 ponent is an element of the intel-  
18 ligence community, that the Assistant  
19 Secretary of Commerce for Commu-  
20 nications and Information, in con-  
21 sultation with such head, determines  
22 would materially assist in the activi-  
23 ties of the working group.

24 (iv) Not fewer than 6 and not more  
25 than 10 experts appointed by the Assistant

1 Secretary of Commerce for Communica-  
2 tions and Information from among the fol-  
3 lowing:

4 (I) Academic institutions.

5 (II) Telecommunications trade  
6 associations, including at least 1 trade  
7 association representing private sector  
8 telecommunications entities that are  
9 small entities.

10 (III) Private sector telecommuni-  
11 cations entities.

12 (IV) Any other entity that the  
13 Assistant Secretary of Commerce for  
14 Communications and Information de-  
15 termines appropriate.

16 (B) SECURITY CLEARANCE AND OTHER  
17 REQUIREMENTS.—

18 (i) UNITED STATES GOVERNMENT EN-  
19 TITY MEMBERS.—The head of a United  
20 States Government entity described in  
21 clause (i), (ii), or (iii) of subparagraph (A)  
22 may only designate under such subpara-  
23 graph an individual who is a senior-level  
24 employee (or an individual occupying a  
25 Senior Executive Service position, as de-

1            fined in section 3132(a) of title 5, United  
2            States Code) at such entity and who is eli-  
3            gible to receive a security clearance that al-  
4            lows for access to sensitive compartmented  
5            information.

6            (ii) OTHER EXPERTS.—The Assistant  
7            Secretary of Commerce for Communica-  
8            tions and Information may not appoint an  
9            individual under subparagraph (A)(iv) un-  
10          less such individual is eligible to receive a  
11          security clearance that allows for access to  
12          sensitive compartmented information.

13          (3) EXECUTIVE BOARD.—

14          (A) COMPOSITION.—The working group  
15          shall have an executive board that consists of  
16          the following:

17                  (i) The Chair and Ranking Member of  
18                  the Committee on Energy and Commerce  
19                  of the House of Representatives.

20                  (ii) The Chair and Ranking Member  
21                  of the Subcommittee on Communications  
22                  and Technology of the Committee on En-  
23                  ergy and Commerce of the House of Rep-  
24                  resentatives.

1 (iii) The Chair and Ranking Member  
2 of the Committee on Homeland Security of  
3 the House of Representatives.

4 (iv) The Chair and Ranking Member  
5 of the Subcommittee on Cybersecurity and  
6 Infrastructure Protection of the Committee  
7 on Homeland Security of the House of  
8 Representatives.

9 (v) The Chair and Ranking Member  
10 of the Permanent Select Committee on In-  
11 telligence of the House of Representatives.

12 (vi) The Chair and Ranking Member  
13 of the Committee on Commerce, Science,  
14 and Transportation of the Senate.

15 (vii) The Chair and Ranking Member  
16 of the Subcommittee on Communications,  
17 Media, and Broadband of the Committee  
18 on Commerce, Science, and Transportation  
19 of the Senate.

20 (viii) The Chair and Ranking Member  
21 of the Select Committee on Intelligence of  
22 the Senate.

23 (ix) The Chair and Ranking Member  
24 of the Committee on Homeland Security  
25 and Governmental Affairs of the Senate.

1           (x) The Chair and Ranking Member  
2 of the Subcommittee on Emerging Threats  
3 and Spending Oversight of the Committee  
4 on Homeland Security and Governmental  
5 Affairs of the Senate.

6           (B) MEETINGS.—

7           (i) IN GENERAL.—During the 1-year  
8 period preceding the date on which each  
9 report required by subsection (b) is trans-  
10 mitted, the working group shall hold at  
11 least 2 meetings before the executive board  
12 established under subparagraph (A) in  
13 which the working group shall share and  
14 analyze the findings and recommendations  
15 to be included in such report.

16           (ii) TIMING.—Of the meetings held  
17 under clause (i) with respect to a report—

18           (I) 1 such meeting shall be held  
19 not later than 240 days before the  
20 date on which such report is trans-  
21 mitted; and

22           (II) 1 such meeting shall be held  
23 not later than 120 days after the date  
24 on which the meeting described in  
25 subclause (I) is held.

1 (b) ANNUAL REPORTS.—

2 (1) REQUIREMENT.—Not later than 1 year  
3 after the date of the enactment of this Act, and an-  
4 nually thereafter for 5 years, the Assistant Secretary  
5 of Commerce for Communications and Information,  
6 in consultation with the Director of the Cybersecu-  
7 rity and Infrastructure Security Agency, shall trans-  
8 mit to the appropriate congressional committees,  
9 each member of the executive board established  
10 under subsection (a)(3)(A), and the Governor of  
11 each State a report—

12 (A) assessing the challenges of protecting  
13 military and commercial telecommunications  
14 networks in the United States from security  
15 threats related to the Signaling System 7 tele-  
16 communication protocol standard (in this sec-  
17 tion referred to as the “SS7 protocol”) posed  
18 by foreign countries of concern and foreign en-  
19 tities of concern; and

20 (B) examining the roles and responsibil-  
21 ities of the United States Government and pri-  
22 vate sector telecommunications entities (includ-  
23 ing small entities) in redressing vulnerabilities  
24 in the SS7 protocol from cybersecurity threats,



1           espionage, vandalism, sabotage, and terrorist or  
2           “lone wolf” activities.

3           (2) MATTERS TO BE INCLUDED.—Each report  
4           under paragraph (1) shall include a description of  
5           the following:

6                   (A) Past, ongoing, or planned efforts by  
7                   the United States Government entities that are  
8                   represented by members of the working group  
9                   described in clauses (i), (ii), and (iii) of sub-  
10                  section (a)(2)(A) to protect telecommunications  
11                  networks in the United States from cybersecu-  
12                  rity threats, espionage, vandalism, sabotage,  
13                  and terrorist or “lone wolf” activities related to  
14                  vulnerabilities in the SS7 protocol.

15                  (B) The capabilities of foreign countries of  
16                  concern and foreign entities of concern to target  
17                  and compromise telecommunications networks  
18                  in the United States through vulnerabilities in  
19                  the SS7 protocol or to intercept data trans-  
20                  missions or sensitive information originating on  
21                  such networks as a result of such  
22                  vulnerabilities.

23                  (C) The risks related to vulnerabilities in  
24                  the SS7 protocol (including an associated as-  
25                  sessment) posed to telecommunications net-

1 works in the United States by foreign countries  
2 of concern and foreign entities of concern, and  
3 the extent to which the United States Govern-  
4 ment entities that are represented by members  
5 of the working group described in clauses (i),  
6 (ii), and (iii) of subsection (a)(2)(A) and private  
7 sector telecommunications entities (including  
8 small entities) may mitigate such risks.

9 (D) Past, ongoing, or planned actions of  
10 the United States Government entities that are  
11 represented by members of the working group  
12 described in clauses (i), (ii), and (iii) of sub-  
13 section (a)(2)(A) to conduct outreach to allies  
14 and partners of the United States relating to  
15 countering the security threats posed to tele-  
16 communications networks by vulnerabilities in  
17 the SS7 protocol.

18 (E) Current mechanisms in place within  
19 the United States Government entities that are  
20 represented by members of the working group  
21 described in clauses (i), (ii), and (iii) of sub-  
22 section (a)(2)(A) and private sector tele-  
23 communications entities (including small enti-  
24 ties) to detect, prevent, suppress, investigate,  
25 mitigate, and respond to any unusual or mali-

1           cious activity resulting from vulnerabilities in  
2           the SS7 protocol and affecting telecommuni-  
3           cations networks in the United States.

4           (F) The resources required for the United  
5           States Government entities that are represented  
6           by members of the working group described in  
7           clauses (i), (ii), and (iii) of subsection (a)(2)(A)  
8           to initiate new, or expand existing, operations  
9           to protect telecommunications networks in the  
10          United States from acts of espionage that ex-  
11          ploit vulnerabilities in the SS7 protocol.

12          (G) Recommendations for initiating new,  
13          or expanding existing, operations by the United  
14          States Government entities that are represented  
15          by members of the working group described in  
16          clauses (i), (ii), and (iii) of subsection (a)(2)(A)  
17          to protect telecommunications networks in the  
18          United States from acts of espionage that ex-  
19          ploit vulnerabilities in the SS7 protocol, includ-  
20          ing an assessment of the feasibility of the fol-  
21          lowing:

22                 (i) Establishing an interagency and  
23                 public-private coordination mechanism to  
24                 ensure that best practices and security rec-  
25                 ommendations released by the working

1 group are distributed to all private sector  
2 telecommunications entities in the United  
3 States.

4 (ii) Training a dedicated intelligence  
5 officer or analyst cadre of the Department  
6 of Homeland Security composed of tele-  
7 communications protocol experts to protect  
8 telecommunications networks in the United  
9 States from such acts.

10 (H) Recommendations for the United  
11 States Government entities that are represented  
12 by members of the working group described in  
13 clauses (i), (ii), and (iii) of subsection (a)(2)(A)  
14 and private sector telecommunications entities  
15 (including small entities) to jointly develop and  
16 establish standards, guidelines, best practices,  
17 methodologies, procedures, or processes to en-  
18 sure the security and integrity of telecommuni-  
19 cations networks in the United States with re-  
20 spect to vulnerabilities in the SS7 protocol.

21 (3) FORM.—Each report under paragraph (1)  
22 shall be transmitted in classified form, but may in-  
23 clude an unclassified annex.

24 (c) BRIEFINGS.—Not later than 30 days after the  
25 date on which each report under subparagraph (b) is

1 transmitted, the working group shall provide to the appro-  
2 priate congressional committees a briefing on the findings  
3 and recommendations contained in such report.

4 (d) DEFINITIONS.—In this section:

5 (1) APPROPRIATE CONGRESSIONAL COMMIT-  
6 TEES.—The term “appropriate congressional com-  
7 mittees” means—

8 (A) the Committee on Homeland Security,  
9 the Committee on Energy and Commerce, and  
10 the Permanent Select Committee on Intelligence  
11 of the House of Representatives; and

12 (B) the Committee on Homeland Security  
13 and Governmental Affairs, the Committee on  
14 Commerce, Science, and Transportation, and  
15 the Select Committee on Intelligence of the  
16 Senate.

17 (2) CYBERSECURITY THREAT.—The term “cy-  
18 bersecurity threat” has the meaning given such term  
19 in section 2200 of the Homeland Security Act of  
20 2002 (6 U.S.C. 650).

21 (3) FOREIGN COUNTRY OF CONCERN.—The  
22 term “foreign country of concern” has the meaning  
23 given such term in section 9901 of the William M.  
24 (Mac) Thornberry National Defense Authorization  
25 Act for Fiscal Year 2021 (15 U.S.C. 4651).

1           (4) FOREIGN ENTITY OF CONCERN.—The term  
2           “foreign entity of concern” has the meaning given  
3           such term in section 9901 of the William M. (Mac)  
4           Thornberry National Defense Authorization Act for  
5           Fiscal Year 2021 (15 U.S.C. 4651).

6           (5) INTELLIGENCE COMMUNITY.—The term  
7           “intelligence community” has the meaning given  
8           such term in section 3(4) of the National Security  
9           Act of 1947 (50 U.S.C. 3003(4)).

10          (6) SMALL ENTITY.—The term “small entity”  
11          means an entity that has fewer than 200 employees.

12          (7) STATE.—The term “State” means each  
13          State of the United States, the District of Columbia,  
14          each commonwealth, territory, or possession of the  
15          United States, and each federally recognized Indian  
16          Tribe.