.....

(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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Securing Every Vector, Enhancing Networks Act'' or the ''SEVEN Act''.

SEC. 2. SS7 INTERAGENCY WORKING GROUP AND REPORT ON ENSURING THE SECURITY AND INTEGRITY OF TELECOMMUNICATIONS NETWORKS.

(a) SS7 INTERAGENCY WORKING GROUP.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Assistant Secretary of Commerce for Communications and Information, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall convene an interagency working group (in this section referred to as the ''working group'') to prepare the annual reports under subsection (b) and provide the briefings under subsection (c).

(2) MEMBERSHIP.—

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

(i) The Assistant Secretary of Commerce for Communications and Information (or the designee of the Assistant Secretary), who shall serve as the Chair of the working group.

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

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

(I) The Secretary of Homeland Security.

(II) The Director of the National Institute of Standards and Technology.

(III) The Chief of Space Operations.

(IV) The Attorney General.

(V) The Secretary of Defense.

(VI) The Chair of the Federal Communications Commission.

(VII) The head of any other component of the United States Government, regardless of whether such component is an element of the intelligence community, that the Assistant Secretary of Commerce for Communications and Information, in consultation with such head, determines would materially assist in the activities of the working group.

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

Secretary of Commerce for Communications and Information from among the following:

(I) Academic institutions.

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

(III) Private sector telecommunications entities.

(IV) Any other entity that the Assistant Secretary of Commerce for Communications and Information determines appropriate.

(B) SECURITY CLEARANCE AND OTHER REQUIREMENTS.—

(i) UNITED STATES GOVERNMENT ENTITY MEMBERS.—The head of a United States Government entity described in clause (i), (ii), or (iii) of subparagraph (A) may only designate under such subparagraph an individual who is a senior-level employee (or an individual occupying a Senior Executive Service position, as de-

fined in section 3132(a) of title 5, United States Code) at such entity and who is eligible to receive a security clearance that allows for access to sensitive compartmented information.

(ii) OTHER EXPERTS.—The Assistant Secretary of Commerce for Communications and Information may not appoint an individual under subparagraph (A)(iv) unless such individual is eligible to receive a security clearance that allows for access to sensitive compartmented information.

(3) EXECUTIVE BOARD.—

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

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

(ii) The Chair and Ranking Member of the Subcommittee on Communications and Technology of the Committee on Energy and Commerce of the House of Representatives.

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

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

(v) The Chair and Ranking Member of the Permanent Select Committee on Intelligence of the House of Representatives.

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

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

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

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

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

(B) MEETINGS.—

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

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

(I) 1 such meeting shall be held not later than 240 days before the date on which such report is transmitted; and

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

(b) ANNUAL REPORTS.—

(1) REQUIREMENT.—Not later than 1 year after the date of the enactment of this Act, and annually thereafter for 5 years, the Assistant Secretary of Commerce for Communications and Information, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall transmit to the appropriate congressional committees, each member of the executive board established under subsection (a)(3)(A), and the Governor of each State a report—

(A) assessing 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 (in this section referred to as the ''SS7 protocol'') posed by foreign countries of concern and foreign entities of concern; and

(B) examining the roles and responsibilities of the United States Government and private sector telecommunications entities (including small entities) in redressing vulnerabilities in the SS7 protocol from cybersecurity threats,

espionage, vandalism, sabotage, and terrorist or ''lone wolf'' activities.

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

(A) Past, ongoing, or planned efforts by the United States Government entities that are represented by members of the working group described in clauses (i), (ii), and (iii) of subsection (a)(2)(A) to protect telecommunications networks in the United States from cybersecurity threats, espionage, vandalism, sabotage, and terrorist or ''lone wolf'' activities related to vulnerabilities in the SS7 protocol.

(B) The capabilities of foreign countries of concern and foreign entities of concern to target and compromise telecommunications networks in the United States through vulnerabilities in the SS7 protocol or to intercept data transmissions or sensitive information originating on such networks as a result of such vulnerabilities.

(C) The risks related to vulnerabilities in the SS7 protocol (including an associated assessment) posed to telecommunications net-

works in the United States by foreign countries of concern and foreign entities of concern, and the extent to which the United States Government entities that are represented by members of the working group described in clauses (i), (ii), and (iii) of subsection (a)(2)(A) and private sector telecommunications entities (including small entities) may mitigate such risks.

(D) Past, ongoing, or planned actions of the United States Government entities that are represented by members of the working group described in clauses (i), (ii), and (iii) of subsection (a)(2)(A) to conduct outreach to allies and partners of the United States relating to countering the security threats posed to telecommunications networks by vulnerabilities in the SS7 protocol.

(E) Current mechanisms in place within the United States Government entities that are represented by members of the working group described in clauses (i), (ii), and (iii) of subsection (a)(2)(A) and private sector telecommunications entities (including small entities) to detect, prevent, suppress, investigate, mitigate, and respond to any unusual or mali-

cious activity resulting from vulnerabilities in the SS7 protocol and affecting telecommunications networks in the United States.

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

(G) Recommendations for initiating new, or expanding existing, operations by the United States Government entities that are represented by members of the working group described in clauses (i), (ii), and (iii) of subsection (a)(2)(A) to protect telecommunications networks in the United States from acts of espionage that exploit vulnerabilities in the SS7 protocol, including an assessment of the feasibility of the following:

(i) Establishing an interagency and public-private coordination mechanism to ensure that best practices and security recommendations released by the working

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

(ii) Training a dedicated intelligence officer or analyst cadre of the Department of Homeland Security composed of telecommunications protocol experts to protect telecommunications networks in the United States from such acts.

(H) Recommendations for the United States Government entities that are represented by members of the working group described in clauses (i), (ii), and (iii) of subsection (a)(2)(A) and private sector telecommunications entities (including small entities) to jointly develop and establish standards, guidelines, best practices, methodologies, procedures, or processes to ensure the security and integrity of telecommunications networks in the United States with respect to vulnerabilities in the SS7 protocol.

(3) FORM.—Each report under paragraph (1) shall be transmitted in classified form, but may include an unclassified annex.

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

transmitted, the working group shall provide to the appropriate congressional committees a briefing on the findings and recommendations contained in such report.

(d) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

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

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

(2) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' has the meaning given such term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

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

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

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

(6) SMALL ENTITY.—The term ''small entity'' means an entity that has fewer than 200 employees.

(7) STATE.—The term ''State'' means each State of the United States, the District of Columbia, each commonwealth, territory, or possession of the United States, and each federally recognized Indian Tribe.