Blackburn - 1 (as modified)

OLL19662 S.L.C.

Marsha Blackburn

AMENDMENT NO._____ Calendar No._____

Purpose: To improve the amendment relating to information sharing.

IN THE SENATE OF THE UNITED STATES—116th Cong., 1st Sess.

S. 1625

To promote the deployment of commercial fifth-generation mobile networks and the sharing of information with communications providers in the United States regarding security risks to the networks of those providers, and for other purposes.

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT intended to be proposed by Mrs. BLACKBURN to the amendment (No. _____) proposed by Mrs. BLACKBURN

Viz:

In lieu of the matter proposed to be inserted, insert the following:

SEC. 8. INFORMATION SHARING WITH COMMUNICATIONS PROVIDERS AND TRUSTED SUPPLIERS.

(a) ESTABLISHMENT OF JOINT PROGRAM.—Not later than 90 days after the date of enactment of this Act, the Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Director of the Federal Bureau of Investigation, the Secretary of Com-

merce, and the Chairman of the Commission, shall establish a joint program to share information regarding security risks, and vulnerabilities related to communications networks and related equipment and services with United States communication providers and trusted suppliers.

(b) DUTIES OF PROGRAM.—The program established under subsection (a) shall—

(1) conduct regular briefings and other events to share information with United States communications providers and trusted suppliers regarding security risks, and vulnerabilities related to communications networks and related equipment and services;

(2) prioritize engagement with United States communications providers that—

(A) are small business concerns (as defined in section 3(a) of the Small Business Act (15 U.S.C. 632(a)); or

(B) primarily serve rural areas;

(3) as determined appropriate and necessary by the Secretary of Homeland Security, facilitate information sharing with United States communications providers and trusted suppliers by providing temporary, security clearances to selected citizens of the United States, limited solely to the information under this section;

(4) develop recommendations for United States communications providers and trusted suppliers to better secure their networks, equipment, and supply chain;

(5) as determined appropriate by the Commission, in consultation with the Assistant Secretary of Commerce for Communications and Information, convene a working group of United States communications providers to engage in discussions and information sharing regarding specific national security risks posed to communications networks; and

(6) ensure that information shared with private entities under this subsection is presented in a manner that identifies, assesses, and prioritizes risks, the mitigation of risks, and opportunities for asymmetric advantage.

(c) VOLUNTARY AND CONFIDENTIAL NATURE OF RECOMMENDATIONS.—

(1) IN GENERAL.—Recommendations developed and provided to communications providers shall be entirely advisory and shall create no obligation on or expectation of communications providers or other non-Federal entities to take any action or abstain from any action.

(2) EXEMPT FROM DISCLOSURE.—Recommendations and briefings created by the joint program created under this section shall be exempt from public disclosure.

(d) AUTHORIZATION TO SHARE.—Notwithstanding any other provision of law, a non-Federal entity participating in the program established under subsection (a) may share with, or receive from, any other non-Federal entity or the Federal Government information regarding security, risks, and vulnerabilities related to communications networks and supply chains.

(e) CONFIDENTIALITY.—Any information shared by non-Federal entities in the program established under this section shall be—

(1) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, Tribal, or local provision of law requiring disclosure of information or records;

(2) withheld, without discretion, from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, Tribal, or local provision of law requiring disclosure of information or records; and

(3) considered the equivalent of Protected Critical Infrastructure Information, as defined and pro-

tected in the Critical Infrastructure Information Act of 2002 and Procedures for Handling Protected Critical Infrastructure Information regulations, promulgated by Department of Homeland Security under part 29 of title 6, Code of Federal Regulations, to provide non-Federal entities confidence that sharing their information with the Government will not expose sensitive or proprietary data.

(f) LAWFUL RESTRICTION ON USE.—

(1) IN GENERAL.—A non-Federal entity receiving information regarding security, risks, and vulnerabilities from another non-Federal entity or a Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such by the sharing non-Federal entity or Federal entity.

(2) PERMITTED USE.—A Federal entity receiving information regarding security, risks, and vulnerabilities from non-Federal entities participating in the program established under this section shall only use that information for the purposes established under this section and in furtherance of the goals of the joint program, and may not release or share the information with other government officials or agencies that are not part of the joint program.

(g) ANTITRUST EXEMPTION.—It shall not be considered a violation of any provision of antitrust laws for 2 or more non-Federal entities to exchange or provide information regarding security, risks, and vulnerabilities under the program established under this section.

(h) PROTECTION FROM LIABILITY.—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the sharing or receipt of information regarding security, risks, and vulnerabilities under the program established under this section.

(i) NO RIGHT, BENEFIT, OR DUTY.—

(1) IN GENERAL.—The sharing of information regarding security, risks, and vulnerabilities with a non-Federal entity in the program established under this section shall not create a right or benefit to similar information by such non-Federal entity or any other non-Federal entity.

(2) RECOMMENDATIONS.—The creation of recommendations by the joint program is not intended to confer any benefits or rights in any party, nor is it intended to create any obligation or duty on any non-Federal entity to take any action or refrain from taking any action.