

Amendment to Rules Committee Print 119-33

Offered by Mr. Ogles of Tennessee

At the end of subtitle B of title XV, insert the following:

SEC. ____. REQUIREMENT FOR MEMORANDA OF AGREEMENT REGARDING VULNERABILITY DISCLOSURE AND PROHIBITION ON PROCUREMENT FROM IT PROVIDERS WHO SHARE CYBER VULNERABILITIES WITH COUNTRIES OF CONCERN.

- (a) REQUIREMENT.—Beginning 270 days after the date of the enactment of this Act, the Secretary of Defense shall not enter into or renew a contract for information technology with any entity which makes such technology commercially available to customers in a country of concern or has operations, subsidiaries, or personnel located in a country of concern unless such entity has entered into a memorandum of agreement with the Department of Defense in accordance with subsection (b).
- (b) MEMORANDUM OF AGREEMENT.—the Secretary of Defense shall require an entity covered under subsection (a) to agree to a memorandum of agreement under which the entity shall—
- (1) disclose all security vulnerabilities affecting procured products or services to the Department of Defense prior to disclosure to any other person or entity, including through a trusted partners program; and
 - (2) not provide advance disclosure of such vulnerabilities to any procured company or entity subject to the control of, or organized under the laws of, a country of concern.
- (c) DEFINITIONS.—In this section:
- (1) ADVANCED DISCLOSURE.—The term “advanced disclosure” means any action that preemptively and privately discloses information pertaining to security vulnerabilities to a select number of entities before publicly making such information available to the general public, including through a trusted partners program.
 - (2) CONTROL.—The term “control” means the power, direct or indirect, whether or not exercised, to determine, direct, dictate, or decide important matters affecting an entity, including through—
 - (A) the ownership of at least 20 percent of the total outstanding voting interest in an entity;
 - (B) board representation;
 - (C) the ability to appoint or discharge any board members, officers, directors, employees, or contractors;
 - (D) proxy voting, a special share, contractual arrangements, legal obligations, formal or informal arrangements to act in concert; or
 - (E) other means.

- (3) COUNTRY OF CONCERN.—The term “country of concern” has the meaning given the term “covered nation” in section 4872(f) of title 10, United States Code.
- (4) COVERED COMPANIES.—The term “covered companies” means—
- (A) any entity owned or operated in whole or in part by a country of concern, or subject to the control of such country of concern, and any subsidiary or parent of such person;
 - or
 - (B) any entity organized under the laws of a country of concern, or having its principal place of business in a country of concern, and any subsidiary of any such person.
- (5) INFORMATION TECHNOLOGY.—The term “information technology” has the meaning given the term in section 11101 of title 40.
- (6) OWNED OR OPERATED IN WHOLE OR IN PART.—The term “owned or operated in whole or in part” means that a foreign country of concern—
- (A) for a person that is a publicly traded company, has the ability to control the company, has access to any material nonpublic technical information in the possession of the company, or has any other rights or involvement in directing, dictating, controlling, or participating in the decision-making of the company beyond those available to a retail investor holding an equivalent share of ownership; and
 - (B) for a person that is a privately held company, has any share of ownership of such company.
- (7) SECURITY VULNERABILITY.—The term “security vulnerability” has the meaning given the term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).
- (8) TRUSTED PARTNERS PROGRAM.—The term “trusted partners program” means any initiative or program run by an information technology provider to provide advanced warnings of security vulnerabilities to defensive security providers for the purpose of helping such providers proactively develop defenses against such vulnerabilities.
- (d) WAIVER.—The Secretary of Defense may waive the requirement under subsection (a) on a case-by-case basis if the Secretary certifies, in writing, to the congressional defense committees that the procurement action is required in the national interest of the United States.