I

112TH CONGRESS
1ST SESSION

H. R. 3523

To provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

NOVEMBER 30, 2011

Mr. ROGERS of Michigan (for himself, Mr. RUPPERSBERGER, Mr. KING of New York, Mr. UPTON, Mrs. MYRICK, Mr. LANGEVIN, Mr. CONAWAY, Mr. MILLER of Florida, Mr. BOREN, Mr. LOBIONDO, Mr. CHANDLER, Mr. NUNES, Mr. GUTIERREZ, Mr. WESTMORELAND, Mrs. BACHMANN, Mr. ROONEY, Mr. HECK, Mr. DICKS, Mr. MCCAUL, Mr. WALDEN, Mr. CALVERT, Mr. SHIMKUS, Mr. TERRY, Mr. BURGESS, Mr. GINGREY of Georgia, Mr. THOMPSON of California, Mr. KINZINGER of Illinois, Mr. AMODEI, and Mr. POMPEO) introduced the following bill; which was referred to the Select Committee on Intelligence (Permanent Select)

A BILL

To provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, 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 ''Cyber Intelligence Sharing and Protection Act of 2011''.

SEC. 2. CYBER THREAT INTELLIGENCE AND INFORMATION SHARING.

(a) IN GENERAL.—Title XI of the National Security Act of 1947 (50 U.S.C. 442 et seq.) is amended by adding at the end the following new section:

''CYBER THREAT INTELLIGENCE AND INFORMATION SHARING

''SEC. 1104. (a) INTELLIGENCE COMMUNITY SHARING OF CYBER THREAT INTELLIGENCE WITH PRIVATE SECTOR.—

''(1) IN GENERAL.—The Director of National Intelligence shall establish procedures to allow elements of the intelligence community to share cyber threat intelligence with private-sector entities and to encourage the sharing of such intelligence.

''(2) SHARING AND USE OF CLASSIFIED INTELLIGENCE.—The procedures established under paragraph (1) shall provide that classified cyber threat intelligence may only be—

''(A) shared by an element of the intelligence community with—

''(i) certified entities; or

''(ii) a person with an appropriate security clearance to receive such cyber threat intelligence;

''(B) shared consistent with the need to protect the national security of the United States; and

''(C) used by a certified entity in a manner which protects such cyber threat intelligence from unauthorized disclosure.

''(3) SECURITY CLEARANCE APPROVALS.—The Director of National Intelligence shall issue guidelines providing that the head of an element of the intelligence community may, as the head of such element considers necessary to carry out this subsection—

''(A) grant a security clearance on a temporary or permanent basis to an employee or officer of a certified entity;

''(B) grant a security clearance on a temporary or permanent basis to a certified entity and approval to use appropriate facilities; and

''(C) expedite the security clearance process for a person or entity as the head of such element considers necessary, consistent with the need to protect the national security of the United States.

''(4) NO RIGHT OR BENEFIT.—The provision of information to a private-sector entity under this sub-

section shall not create a right or benefit to similar information by such entity or any other private-sector entity.

''(b) PRIVATE SECTOR USE OF CYBERSECURITY SYSTEMS AND SHARING OF CYBER THREAT INFORMATION.—

''(1) IN GENERAL.—

''(A) CYBERSECURITY PROVIDERS.—Notwithstanding any other provision of law, a cybersecurity provider, with the express consent of a protected entity for which such cybersecurity provider is providing goods or services for cybersecurity purposes, may, for cybersecurity purposes—

''(i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such protected entity; and

''(ii) share such cyber threat information with any other entity designated by such protected entity, including, if specifically designated, the Federal Government.

''(B) SELF-PROTECTED ENTITIES.—Notwithstanding any other provision of law, a self-protected entity may, for cybersecurity purposes—

"(i) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property of such self-protected entity; and

"(ii) share such cyber threat information with any other entity, including the Federal Government.

"(2) USE AND PROTECTION OF INFORMATION.—Cyber threat information shared in accordance with paragraph (1)—

"(A) shall only be shared in accordance with any restrictions placed on the sharing of such information by the protected entity or self-protected entity authorizing such sharing, including, if requested, appropriate anonymization or minimization of such information;

"(B) may not be used by an entity to gain an unfair competitive advantage to the detriment of the protected entity or the self-protected entity authorizing the sharing of information; and

"(C) if shared with the Federal Government—

''(i) shall be exempt from disclosure under section 552 of title 5, United States Code;

''(ii) shall be considered proprietary information and shall not be disclosed to an entity outside of the Federal Government except as authorized by the entity sharing such information; and

''(iii) shall not be used by the Federal Government for regulatory purposes.

''(3) EXEMPTION FROM LIABILITY.—No civil or criminal cause of action shall lie or be maintained in Federal or State court against a protected entity, self-protected entity, cybersecurity provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, acting in good faith—

''(A) for using cybersecurity systems or sharing information in accordance with this section; or

''(B) for not acting on information obtained or shared in accordance with this section.

''(4) RELATIONSHIP TO OTHER LAWS REQUIRING THE DISCLOSURE OF INFORMATION.—The sub-

mission of information under this subsection to the Federal Government shall not satisfy or affect any requirement under any other provision of law for a person or entity to provide information to the Federal Government.

''(c) REPORT ON INFORMATION SHARING.—The Privacy and Civil Liberties Oversight Board established under section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (5 U.S.C. 601 note) shall annually submit to Congress a report in unclassified form containing—

''(1) a review of the sharing and use of information by the Federal Government under this section and the procedures and guidelines established or issued by the Director of National Intelligence under subsection (a); and

''(2) any recommendations of the Board for improvements or modifications to such authorities to address privacy and civil liberties concerns.

''(d) FEDERAL PREEMPTION.—This section supersedes any statute of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under subsection (b).

''(e) SAVINGS CLAUSE.—Nothing in this section shall be construed to limit any other authority to use a cyberse-

curity system or to identify, obtain, or share cyber threat intelligence or cyber threat information.

''(f) DEFINITIONS.—In this section:

''(1) CERTIFIED ENTITY.—The term 'certified entity' means a protected entity, self-protected entity, or cybersecurity provider that—

''(A) possesses or is eligible to obtain a security clearance, as determined by the Director of National Intelligence; and

''(B) is able to demonstrate to the Director of National Intelligence that such provider or such entity can appropriately protect classified cyber threat intelligence.

''(2) CYBER THREAT INTELLIGENCE.—The term 'cyber threat intelligence' means information in the possession of an element of the intelligence community directly pertaining to a vulnerability of, or threat to, a system or network of a government or private entity, including information pertaining to the protection of a system or network from—

''(A) efforts to degrade, disrupt, or destroy such system or network; or

''(B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information.

''(3) CYBERSECURITY PROVIDER.—The term 'cybersecurity provider' means a non-governmental entity that provides goods or services intended to be used for cybersecurity purposes.

''(4) CYBERSECURITY PURPOSE.—The term 'cybersecurity purpose' means the purpose of ensuring the integrity, confidentiality, or availability of, or safeguarding, a system or network, including protecting a system or network from—

''(A) efforts to degrade, disrupt, or destroy such system or network; or

''(B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information.

''(5) CYBERSECURITY SYSTEM.—The term 'cybersecurity system' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or safeguard, a system or network, including protecting a system or network from—

''(A) efforts to degrade, disrupt, or destroy such system or network; or

''(B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information.

''(6) CYBER THREAT INFORMATION.—The term 'cyber threat information' means information directly pertaining to a vulnerability of, or threat to a system or network of a government or private entity, including information pertaining to the protection of a system or network from—

''(A) efforts to degrade, disrupt, or destroy such system or network; or

''(B) theft or misappropriation of private or government information, intellectual property, or personally identifiable information.

''(7) PROTECTED ENTITY.—The term 'protected entity' means an entity, other than an individual, that contracts with a cybersecurity provider for goods or services to be used for cybersecurity purposes.

''(8) SELF-PROTECTED ENTITY.—The term 'self-protected entity' means an entity, other than an individual, that provides goods or services for cybersecurity purposes to itself.''.

(b) PROCEDURES AND GUIDELINES.—The Director of National Intelligence shall—

(1) not later than 60 days after the date of the enactment of this Act, establish procedures under paragraph (1) of section 1104(a) of the National Se-

curity Act of 1947, as added by subsection (a) of this section, and issue guidelines under paragraph (3) of such section 1104(a); and

(2) following the establishment of such procedures and the issuance of such guidelines, expeditiously distribute such procedures and such guidelines to appropriate Federal Government and private-sector entities.

(c) INITIAL REPORT.—The first report required to be submitted under subsection (c) of section 1104 of the National Security Act of 1947, as added by subsection (a) of this section, shall be submitted not later than one year after the date of the enactment of this Act.

(d) TABLE OF CONTENTS AMENDMENT.—The table of contents in the first section of such Act is amended by adding at the end the following new item:

"Sec. 1104. Cyber threat intelligence and information sharing.".

○