I

107TH CONGRESS
1ST SESSION

H. R. 2435

To encourage the secure disclosure and protected exchange of information about cyber security problems, solutions, test practices and test results, and related matters in connection with critical infrastructure protection.

IN THE HOUSE OF REPRESENTATIVES

JULY 10, 2001

Mr. TOM DAVIS of Virginia (for himself, Mr. MORAN of Virginia, Mr. ISAKSON, and Mr. SESSIONS) introduced the following bill; which was referred to the Committee on Government Reform, and in addition to the Committee on the Judiciary, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To encourage the secure disclosure and protected exchange of information about cyber security problems, solutions, test practices and test results, and related matters in connection with critical infrastructure protection.

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 Security Information Act''.

SEC. 2. FINDINGS AND PURPOSES.

(a) FINDINGS.—Congress finds the following:

(1)(A) Many information technology computer systems, software programs, and similar facilities are essential to the functioning of markets, commerce, consumer products, utilities, government, and safety and defense systems, in the United States and throughout the world.

(B) Protecting systems and products against domestic and international attacks or misuse through the Internet, public, or private telecommunications systems, or similar means is a matter of national and global interest.

(C) Such protection is best accomplished through private sector solutions that are market driven and industry led because the private sector owns, operates, and has developed many of the networks, products, and services that constitute the information infrastructure.

(D) Government should work cooperatively with industry on a voluntary basis to achieve such protection and should not mandate the private sector use particular technologies, dictate standards, or impose undue costs.

(2) The prompt, voluntary, candid, and thorough, but secure and protected, disclosure and ex-

change of information related to the cyber security of entities, systems, and infrastructure—

(A) would greatly enhance the ability of private and public entities to improve their cyber security;

(B) would measurably contribute to avoidance of financial risk and loss resulting from disruption or harm to critical institutional elements of the United States economy, including but not limited to securities exchanges, banking and other financial services institutions, communications networks, transportation systems, manufacturing, information technology, health care, government services, and electric utilities and energy providers, or from serious damage to public confidence in such critical institutional elements; and

(C) is therefore a vital factor in minimizing any potential cyber security-related disruption to the Nation's critical infrastructure and the consequences for its economic well-being and national security.

(3) Concern about the potential for legal liability associated with the disclosure and exchange of cyber security information has impeded and con-

tinues to impede the secure disclosure and protected exchange of such information.

(4) The capability to securely disclose and engage in the protected exchange of information relating to cyber security, solutions, test practices, test results, and risk assessments and audits, without undue concern about inappropriate disclosure of that information, is critical to the ability of private and public entities to address cyber security needs in a timely manner.

(5) The national interest will be served by uniform legal standards in connection with the secure disclosure and protected exchange of cyber security information that will promote appropriate disclosures and exchanges of such information in a timely fashion.

(6) The ''National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue'', released by the President on January 7, 2000, calls for the Government to assist in seeking changes to applicable laws on ''Freedom of Information, liability, and antitrust where appropriate'' in order to foster industry-wide centers for information sharing and analysis.

(b) PURPOSES.—Based upon the powers contained in article 1, section 8, clause 3 of the Constitution of the United States, the purposes of this Act are—

(1) to promote the secure disclosure and protected exchange of cyber security information;

(2) to assist private industry and government in responding effectively and rapidly to cyber security problems;

(3) to lessen burdens on interstate commerce by establishing certain legal principles in connection with the secure disclosure and protected exchange of cyber security information; and

(4) to protect the legitimate users of cyber networks and systems, and to protect the privacy and confidentiality of shared information.

SEC. 3. DEFINITIONS.

In this Act:

(1) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given to it in subsection (a) of the first section of the Clayton Act (15 U.S.C. 12(a)), except that such term includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent such

section 5 applies to unfair methods of competition; and

(B) includes any State law with the same intent and effect as the laws referred to in subparagraph (A).

(2) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' means facilities or services so vital to the nation or its economy that their disruption, incapacity, or destruction would have a debilitating impact on the defense, security, long-term economic prosperity, or public health or safety of the United States.

(3) CYBER SECURITY INFORMATION.—

(A) IN GENERAL.—The term ''cyber security information'' means information related to—

(i) the ability of any protected system, or critical infrastructure to resist intentional interference, compromise, or incapacitation through the misuse of or unauthorized access to or use of the Internet, public or private telecommunications systems, or other similar conduct that violates Federal, State, or international law, that harms interstate commerce of the United

States, or that threatens public health or safety;

(ii) any planned or past assessment, projection or estimate concerning a cyber security vulnerability of a protected system, or critical infrastructure;

(iii) any planned or past cyber security testing, risk assessment, or audit;

(iv) any planned or past operational problems or solutions related to the cyber security of any protected system, or critical infrastructure; or

(v) any immediate threats to the cyber security of any protected system, or critical infrastructure.

(B) EXCLUSION.—For the purposes of any action brought under the securities laws, as that term is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47)), the term ''cyber security information'' does not include information or statements contained in any documents or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to section 12(i) of the Securities Exchange

Act of 1934 (15 U.S.C. 781(i)), or disclosures or writing that when made accompanied the solicitation of an offer or sale of securities.

(4) PROTECTED SYSTEM.—The term ''protected system'' includes but is not limited to any system or process deployed in or remotely affecting a critical infrastructure facility consisting of one or more of the following: computer, computer system, network, or any component hardware or element of the foregoing, software program, processing instruction or data in storage, irrespective of the storage medium.

(5) INFORMATION SHARING ORGANIZATION; ISO.—The terms ''Information Sharing Organization'' and ''ISO'' mean an Information Sharing and Analysis Center (''ISAC'') or any other entity created by private sector organizations for the purpose of sharing cyber security information among such organizations, with or among their individual affiliated members, and with and from State, local, and Federal Government agencies.

SEC. 4. PROTECTION FOR CYBER SECURITY INFORMATION SHARED WITH THE GOVERNMENT.

(a) IN GENERAL.—Cyber security information that is voluntarily provided to any Federal entity, agency, or

authority shall not be disclosed and must be protected against disclosure.

(b) SPECIFICS.—This section shall apply to cyber security information voluntarily provided—

(1) directly to the government about its own cyber security;

(2) directly to the government about a third party's cyber security; or

(3) to an ISO, which is subsequently provided to the government in identifiable form.

(c) PROTECTIONS.—Except with the express consent or permission of the provider of cyber security information, any cyber security information provided pursuant to subsection (b)—

(1) shall be exempt from disclosure under section 552(a) of title 5, United States Code (commonly known as the ''Freedom of Information Act''), by any Federal entity, agency, and authority;

(2) shall not be disclosed to any third party except pursuant to subsection (e)(3); and

(3) shall not be used by any Federal or State entity, agency, or authority or by any third party, directly or indirectly, in any civil action arising under any Federal or State law.

(d) EXEMPTIONS.—Any disclosure of cyber security information by any private entity, or by any Information Sharing Organization as defined in section 3(5) of this Act, to any official of an agency of the United States in accordance with subsection (b) of this section shall not be subject to—

(1) the requirements of the Federal Advisory Committee Act (5 U.S.C. App.) with regard to notice of meetings and publication of the record of such disclosure; and

(2) any agency rules regarding ex parte communications with decision making officials.

(e) EXCEPTIONS.—

(1) INFORMATION OBTAINED ELSEWHERE.—Nothing in this section shall preclude a Federal or State entity, agency, or authority, or any third party, from separately obtaining cyber security information through the use of independent legal authorities, and using such separately obtained information in any action.

(2) PUBLIC DISCLOSURE.—A restriction on use or disclosure of information under this section shall not apply to any information disclosed generally or broadly to the public.

(3) THIRD PARTY INFORMATION.—A Federal entity, agency, or authority receiving cyber security information from one private entity about another private entity's cyber security shall notify and convey that information to the latter upon its initial receipt, except that such entity, agency, or authority shall not notify the third party if the Government has probable cause to believe that such party has conducted, or may be conducting economic espionage against United States entities within the meaning of the Economic Espionage Act (18 U.S.C. 1831 et seq.) or if such entity derives support from any nation currently under a trade embargo.

SEC. 5. ANTITRUST EXEMPTION.

(a) EXEMPTION.—Except as provided in subsection (b), the antitrust laws shall not apply to conduct engaged in, including making and implementing an agreement, solely for the purpose of and limited to—

(1) facilitating the correction or avoidance of a cyber security-related problem; or

(2) communication of or disclosing information to help correct or avoid the effects of a cyber security-related program.

(b) EXCEPTION TO EXEMPTION.—Subsection (a) shall not apply with respect to conduct that involves or

results in an agreement to boycott any person, to allocate a market, or to fix prices or output.

SEC. 6. CYBER SECURITY WORKING GROUPS.

(a) IN GENERAL.—

(1) WORKING GROUPS.—The President may establish and terminate working groups composed of Federal employees who will engage outside organizations in discussions to address cyber security, to share information related to cyber security, and otherwise to serve the purposes of this Act.

(2) LIST OF GROUPS.—The President shall maintain and make available to the public a printed and electronic list of such working groups and a point of contact for each, together with an address, telephone number, and electronic mail address for such point of contact.

(3) BALANCE.—The President shall seek to achieve a balance of participation and representation among the working groups.

(4) MEETINGS.—Each meeting of a working group created under this section shall be announced in advance in accordance with procedures established by the President.

(b) FEDERAL ADVISORY COMMITTEE ACT.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the working groups established under this section.

(c) PRIVATE RIGHT OF ACTION.—This section creates no private right of action to sue for enforcement of any provision of this section.

○