

.....
(Original Signature of Member)

106TH CONGRESS
2D SESSION

H. R. _____

IN THE HOUSE OF REPRESENTATIVES

Mr. DAVIS of Virginia (for himself and Mr. MORAN of Virginia) introduced the following bill; which was referred to the Committee on _____

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION. 1. SHORT TITLE.**

4 This Act may be cited as the “Cyber Security Infor-
5 mation Act”.

1 **SEC. 2. FINDINGS AND PURPOSES.**

2 (a) FINDINGS.—Congress finds the following:

3 (1)(A) Many information technology computer
4 systems, software programs, and similar facilities
5 are vulnerable to attacks or misuse through the
6 Internet, public or private telecommunications sys-
7 tems, or similar means.

8 (B) The problem described in subparagraph (A)
9 and resulting failures could incapacitate systems
10 that are essential to the functioning of markets,
11 commerce, consumer products, utilities, government,
12 and safety and defense systems, in the United States
13 and throughout the world.

14 (C) Protecting, reprogramming, or replacing af-
15 fected systems before the problem incapacitates es-
16 sential systems is a matter of national and global in-
17 terest.

18 (2) The prompt, candid, and thorough, but se-
19 cure and protected, disclosure and exchange of infor-
20 mation related to the cybersecurity of entities, sys-
21 tems, and infrastructure—

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

25 (B) is therefore a matter of national im-
26 portance and a vital factor in minimizing any

1 potential cyber security related disruption to
2 the Nation's economic well-being and security.

3 (3) Concern about the potential for legal liabil-
4 ity associated with the disclosure and exchange of
5 cyber security information could unnecessarily im-
6 pede the secure disclosure and protected exchange of
7 such information.

8 (4) The capability to securely disclose and en-
9 gage in the protected exchange of information relat-
10 ing to cyber security, solutions, test practices and
11 test results, without undue concern about inappro-
12 priate disclosure of that information, is critical to
13 the ability of public and private entities to address
14 cyber security needs in a timely manner.

15 (5) The national interest will be served by uni-
16 form legal standards in connection with the secure
17 disclosure and protected exchange of cyber security
18 information that will promote appropriate disclo-
19 sures and exchanges of such information in a timely
20 fashion.

21 (6) The "National Plan for Information Sys-
22 tems Protection, Version 1.0, An Invitation to a
23 Dialogue", released by the President on January 7,
24 2000, calls for the Government to assist in seeking
25 changes to applicable laws on "Freedom of Informa-

1 tion, liability, and antitrust where appropriate” in
2 order to foster industry-wide centers for information
3 sharing and analysis.

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

7 (1) to promote the secure disclosure and pro-
8 tected exchange of information related to cyber secu-
9 rity;

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

13 (3) to lessen burdens on interstate commerce by
14 establishing certain uniform legal principles in con-
15 nection with the secure disclosure and protected ex-
16 change of information related to cyber security; and

17 (4) to protect the legitimate users of cyber net-
18 works and systems, and to protect the privacy and
19 confidence of shared information.

20 **SEC. 3. DEFINITIONS.**

21 In this Act:

22 (1) ANTITRUST LAWS.—The term “antitrust
23 laws”—

24 (A) has the meaning given to it in sub-
25 section (a) of the first section of the Clayton

1 Act (15 U.S.C. 12(a)), except that such term
2 includes section 5 of the Federal Trade Com-
3 mission Act (15 U.S.C. 45) to the extent such
4 section 5 applies to unfair methods of competi-
5 tion; and

6 (B) includes any State law similar to the
7 laws referred to in subparagraph (A).

8 (2) CRITICAL INFRASTRUCTURE.—The term
9 “critical infrastructure” means facilities or services
10 so vital to the nation or its economy that their dis-
11 ruption, incapacity, or destruction would have a de-
12 bilitating impact on the defense, security, long-term
13 economic prosperity, or health or safety of the
14 United States.

15 (3) CYBER SECURITY.—The term “cyber secu-
16 rity” means the vulnerability of any computing sys-
17 tem, software program, or critical infrastructure to,
18 or their ability to resist, intentional interference,
19 compromise, or incapacitation through the misuse
20 of, or by unauthorized means of, the Internet, public
21 or private telecommunications systems, or other
22 similar conduct that violates Federal, State, or inter-
23 national law, that harms interstate commerce of the
24 United States, or that threatens public health or
25 safety.

1 (4) CYBER SECURITY INTERNET WEBSITE.—
2 The term “cyber security Internet website” means
3 an Internet website or other similar electronically ac-
4 cessible service, clearly designated on the website or
5 service by the person or entity creating or control-
6 ling the content of the website or service as an area
7 where cyber security statements are posted or other-
8 wise made accessible to appropriate entities.

9 (5) CYBER SECURITY STATEMENT.—

10 (A) IN GENERAL.—The term “cyber secu-
11 rity statement” means any communication or
12 other conveyance of information by a party to
13 another, in any form or medium including by
14 means of a cyber security Internet website—

15 (i) concerning an assessment, projec-
16 tion, or estimate concerning the cyber se-
17 curity of that entity, its computer systems,
18 its software programs, or similar facilities
19 of its own;

20 (ii) concerning plans, objectives, or
21 timetables for implementing or verifying
22 the cyber security thereof;

23 (iii) concerning test plans, test dates,
24 test results, or operational problems or so-

1 lutions related to the cyber security there-
2 of; or

3 (iv) reviewing, commenting on, or oth-
4 erwise directly or indirectly relating to the
5 cyber security thereof.

6 (B) NOT INCLUDED.—For the purposes of
7 any action brought under the securities laws, as
8 that term is defined in section 3(a)(47) of the
9 Securities Exchange Act of 1934 (15 U.S.C.
10 78c(a)(47)), the term “cyber security state-
11 ment” does not include statements contained in
12 any documents or materials filed with the Secu-
13 rities and Exchange Commission, or with Fed-
14 eral banking regulators, pursuant to section
15 12(i) of the Securities Exchange Act of 1934
16 (15 U.S.C. 781(i)), or disclosures or writing
17 that when made accompanied the solicitation of
18 an offer or sale of securities.

19 **SEC. 4. SPECIAL DATA GATHERING.**

20 (a) IN GENERAL.—Any Federal entity, agency, or au-
21 thority may expressly designate a request for the vol-
22 untary provision of information relating to cyber security,
23 including cyber security statements, as a cyber security
24 data gathering request made pursuant to this section.

1 (b) SPECIFICS.—A cyber security data gathering re-
2 quest made under this section—

3 (A) shall specify a Federal entity, agency,
4 or authority, or, with its consent, another public
5 or private entity, agency, or authority, to gather
6 responses to the request;

7 (B) shall be a request from a private enti-
8 ty, agency, or authority to a Federal entity,
9 agency, or authority; or

10 (C) shall be deemed to have been made
11 and to have specified such a private entity,
12 agency, or authority when the Federal entity,
13 agency, or authority has voluntarily been given
14 cyber security information gathered by that pri-
15 vate entity, agency, or authority, including by
16 means of a cyber security Internet website.

17 (c) PROTECTIONS.—Except with the express consent
18 or permission of the provider of information described in
19 paragraph (1), any cyber security statements or other
20 such information provided by a party in response to a spe-
21 cial cyber security data gathering request made under this
22 section—

23 (1) shall be exempt from disclosure under sec-
24 tion 552(a) of title 5, United States Code (com-

1 monly known as the “Freedom of Information Act”),
2 by all Federal entities, agencies, and authorities;

3 (2) shall not be disclosed to or by any third
4 party; and

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

9 (d) EXCEPTIONS.—

10 (1) INFORMATION OBTAINED ELSEWHERE.—

11 Nothing in this section shall preclude a Federal enti-
12 ty, agency, or authority, or any third party, from
13 separately obtaining the information submitted in
14 response to a request under this section through the
15 use of independent legal authorities, and using such
16 separately obtained information in any action.

17 (2) PUBLIC DISCLOSURE.—A restriction on use
18 or disclosure of information under this section shall
19 not apply to any information disclosed generally or
20 broadly to the public with the express consent of the
21 party.

22 **SEC. 5. ANTITRUST EXEMPTION.**

23 (a) EXEMPTION.—Except as provided in subsection

24 (b), the antitrust laws shall not apply to conduct engaged

1 in, including making and implementing an agreement,
2 solely for the purpose of and limited to—

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

5 (2) communicating or disclosing information to
6 help correct or avoid the effects of a cyber security
7 related problem.

8 (b) EXCEPTION TO EXEMPTION.—Subsection (a)
9 shall not apply with respect to conduct that involves or
10 results in an agreement to boycott any person, to allocate
11 a market, or to fix prices or output.

12 **SEC. 6. CYBER SECURITY WORKING GROUPS.**

13 (a) IN GENERAL.—

14 (1) WORKING GROUPS.—The President may es-
15 tablish and terminate working groups composed of
16 Federal employees who will engage outside organiza-
17 tions in discussions to address cyber security, to
18 share information related to cyber security, and oth-
19 erwise to serve the purposes of this Act.

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

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

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

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

11 (c) PRIVATE RIGHT OF ACTION.—This section cre-
12 ates no private right of action to sue for enforcement of
13 any provision of this section.