

AMENDMENT NO. _____ Calendar No. _____

Purpose: To facilitate the security of the critical infrastructure of the United States.

IN THE SENATE OF THE UNITED STATES—107th Cong., 1st Sess.

S. _____

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 Mr. BENNETT

Viz:

1 At the appropriate place, insert the following:

2 **TITLE _____—PROTECTION OF**
3 **CRITICAL INFRASTRUCTURE**

4 **SEC. ____ 01. SHORT TITLE.**

5 This title may be cited as the “Critical Infrastructure
6 Information Act of 2001”.

7 **SEC. ____ 02. FINDINGS.**

8 Congress makes the following findings:

9 (1) The critical infrastructures that underpin
10 our society, national defense, economic prosperity,
11 and quality of life—including energy, banking and
12 finance, transportation, vital human services, and

1 telecommunications—must be viewed in a new con-
2 text in the Information Age.

3 (2) The rapid proliferation and integration of
4 telecommunications and computer systems have con-
5 nected infrastructures to one another in a complex
6 global network of interconnectivity and interdepend-
7 ence. Many information technology computer sys-
8 tems, software programs, and similar facilities are
9 critical to the functioning of markets, commerce,
10 consumer products, utilities, government, and safety
11 and defense systems, in the United States and
12 throughout the world. As a result, new
13 vulnerabilities to such systems and infrastructures
14 have emerged, such as the threat of physical and
15 cyber attacks from terrorists or hostile nations.
16 These attacks could disrupt the economy and endan-
17 ger the health, welfare and security of the United
18 States.

19 (3) The private sector, which owns and operates
20 the majority of these critical infrastructures, and the
21 Government, which has unique information and ana-
22 lytical capabilities, both could greatly benefit from
23 cooperating in response to threats, vulnerabilities,
24 and actual attacks to critical infrastructures, by
25 sharing information and analysis.

1 (4) Protecting systems and products against do-
2 mestic and international attacks or misuse through
3 the Internet, public or private telecommunications
4 systems, or similar means is a matter of national
5 and global interest.

6 (5) Such protection is best accomplished
7 through private sector solutions that are market
8 driven and industry led because the private sector
9 owns, operates, and has developed many of the net-
10 works, products, and services that constitute the na-
11 tion's critical infrastructure.

12 (6) Government should work cooperatively with
13 industry on a voluntary basis to achieve such protec-
14 tion and should not mandate the private sector use
15 particular technologies, dictate standards, or impose
16 undue costs.

17 (7) The prompt, voluntary, candid, and thor-
18 ough, but secure and protected, disclosure and ex-
19 change of information related to the security of enti-
20 ties, systems, and infrastructure—

21 (A) would greatly enhance the ability of
22 private and public entities to improve their in-
23 frastructure and cyber security;

24 (B) would measurably contribute to avoid-
25 ance of financial risk and loss resulting from

1 disruption or harm to critical institutional ele-
2 ments of the United States economy (including
3 securities exchanges, banking and other finan-
4 cial services institutions, communications net-
5 works, transportation systems, manufacturing,
6 information technology, health care, government
7 services, and electric utilities and energy pro-
8 viders) or from serious damage to public con-
9 fidence in such critical institutional elements;
10 and

11 (C) is therefore a vital factor in minimizing
12 any potential disruption to the Nation's critical
13 infrastructure and the resulting harm to its
14 health, welfare and security.

15 (8) The private sector is hesitant to share crit-
16 ical infrastructure information with the Government
17 because—

18 (A) Federal law provides no clear assur-
19 ance that critical infrastructure information vol-
20 untarily submitted to the Government will be
21 protected from disclosure or misuse that could
22 result in legal liability or financial harm;

23 (B) the framework of the Government for
24 critical infrastructure information sharing and
25 analysis is not sufficiently developed; and

1 (C) concerns about possible prosecution
2 under the antitrust laws inhibit some companies
3 from partnering with other industry members,
4 including competitors, to develop cooperative in-
5 frastructure security strategies.

6 (9) The capability to securely disclose and en-
7 gage in the protected exchange of information relat-
8 ing to critical infrastructure solutions, test practices,
9 test results, and risk assessments and audits, with-
10 out undue concern about inappropriate disclosure of
11 that information, is critical to the ability of private
12 and public entities to address critical infrastructure
13 needs in a timely manner.

14 (10) The national interest will be served by uni-
15 form legal standards in connection with the secure
16 disclosure and protected exchange of critical infra-
17 structure information that will promote appropriate
18 disclosures and exchanges of such information in a
19 timely fashion.

20 (11) The “National Plan for Information Sys-
21 tems Protection, Version 1.0, An Invitation to a
22 Dialogue”, released by the President on January 7,
23 2000, calls for the Government to assist in seeking
24 changes to applicable laws on “Freedom of Informa-
25 tion, liability, and antitrust where appropriate” in

1 order to foster industry-wide centers for information
2 sharing and analysis.

3 (12) Statutory nondisclosure provisions that
4 qualify as Exemption 3 statutes under section 552
5 of title 5, United States Code (commonly referred to
6 as the Freedom of Information Act), many of them
7 longstanding, prohibit disclosure of numerous classes
8 of information under such section. These statutes
9 cover specific and narrowly defined classes of infor-
10 mation and are consistent with the principles of free
11 and open government that such section seeks to fa-
12 cilitate.

13 (13) Since the infrastructure information that
14 this title covers is not normally in the public domain,
15 preventing public disclosure of this sensitive infor-
16 mation serves the greater good by promoting na-
17 tional security and economic stability.

18 **SEC. ___ 03. PURPOSE.**

19 Based upon the powers contained in article 1, section
20 8, clause 3 of the Constitution of the United States, the
21 purposes of this title are to foster improved security of
22 critical infrastructure by—

23 (1) promoting the increased sharing of critical
24 infrastructure information both among private sector

1 entities, as well as between the Government and the
2 private sector, in a secure and protected manner;

3 (2) encouraging the private sector and the Gov-
4 ernment to conduct and share the results of better
5 analyses of critical infrastructure information in
6 order to prevent, detect, warn of, and respond effec-
7 tively and rapidly to incidents involving critical in-
8 frastructure and protected systems;

9 (3) to lessen burdens on interstate commerce by
10 establishing certain legal principles in connection
11 with the secure disclosure and protected exchange of
12 critical infrastructure information; and

13 (4) to protect the legitimate users and uses of
14 critical infrastructure networks and systems, and to
15 protect the privacy and confidentiality of shared crit-
16 ical infrastructure information.

17 **SEC. ___04. DEFINITIONS.**

18 In this title:

19 (1) **AGENCY.**—The term “agency” has the
20 meaning given it in section 551 of title 5, United
21 States Code.

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

24 (A) has the meaning given it in subsection
25 (a) of the first section of the Clayton Act (15

1 U.S.C. 12(a)), except that such term includes
2 section 5 of the Federal Trade Commission Act
3 (15 U.S.C. 45) to the extent such section 5 ap-
4 plies to unfair methods of competition; and

5 (B) includes any State law with the same
6 intent and effect as the laws referred to in sub-
7 paragraph (A).

8 (3) COVERED FEDERAL AGENCY.—The term
9 “covered Federal agency” means the following:

10 (A) The Department of Justice.

11 (B) The Department of Defense.

12 (C) The Department of Commerce.

13 (D) The Department of Transportation.

14 (E) The Department of the Treasury.

15 (F) The Department of Health and
16 Human Services.

17 (G) The Department of Energy.

18 (H) The Environmental Protection Agency.

19 (I) The General Services Administration.

20 (J) The Federal Communications Commis-
21 sion.

22 (K) The Federal Emergency Management
23 Agency.

24 (L) The National Infrastructure Protection
25 Center.

1 (M) The National Communication System.

2 (N) The Nuclear Regulatory Commission.

3 (4) CRITICAL INFRASTRUCTURE.—The term
4 “critical infrastructure”—

5 (A) means physical, information, and data
6 systems and services essential to the national
7 defense, government, public health or safety, or
8 economy of the United States (including all
9 types of communications and data transmission
10 systems, electric power, gas and oil production,
11 refining, storage, transportation and distribu-
12 tion, banking and finance, transportation, water
13 supply, emergency services (including medical,
14 fire, and police services)), the continuity of gov-
15 ernment operations, and their associated pro-
16 tected or essential systems; and

17 (B) includes any industry sector des-
18 ignated by the President pursuant to the Na-
19 tional Security Act of 1947 (50 U.S.C. 401 et
20 seq.) or the Defense Production Act of 1950
21 (50 U.S.C. App. 2061 et seq.) as essential to
22 provide resources for the execution of the na-
23 tional security strategy of the United States, in-
24 cluding emergency preparedness activities pur-
25 suant to title VI of the Robert T. Stafford Dis-

1 aster Relief and Emergency Assistance Act (42
2 U.S.C. 5195 et seq.).

3 (5) CRITICAL INFRASTRUCTURE INFORMA-
4 TION.—The term “critical infrastructure informa-
5 tion” means information related to—

6 (A) the ability of any critical infrastructure
7 or protected system to resist interference, com-
8 promise, or incapacitation by either physical or
9 computer-based attack or other similar conduct
10 (including the misuse of or unauthorized access
11 to all types of communications and data trans-
12 mission systems) that violates Federal, State,
13 or local law, harms interstate commerce of the
14 United States, or threatens public health or
15 safety;

16 (B) any planned or past assessment, pro-
17 jection, or estimate of the security vulnerability
18 of critical infrastructure or a protected system,
19 including security testing, risk evaluation, risk
20 management planning, or risk audit;

21 (C) any planned or past operational prob-
22 lem or solution, including repair, recovery, re-
23 construction, insurance, or continuity, related to
24 the security of critical infrastructure or a pro-
25 tected system; or

1 (D) any threat to the security of critical
2 infrastructure or a protected system.

3 (6) INFORMATION SHARING AND ANALYSIS OR-
4 GANIZATION.—The term “Information Sharing and
5 Analysis Organization” means any formal or infor-
6 mal entity or collaboration created by public or pri-
7 vate sector organizations, and composed primarily of
8 such organizations, for purposes of—

9 (A) gathering and analyzing critical infra-
10 structure information in order to better under-
11 stand security problems related to critical infra-
12 structure and protected systems, and inter-
13 dependencies of critical infrastructure and pro-
14 tected systems, so as to ensure the availability,
15 integrity, and reliability of critical infrastruc-
16 ture and protected systems;

17 (B) communicating or disclosing critical
18 infrastructure information to help prevent, de-
19 tect, mitigate, or recover from the effects of a
20 problem related to critical infrastructure or pro-
21 tected systems; and

22 (C) voluntarily disseminating critical infra-
23 structure information to its members, State,
24 local, and Federal Governments, or any entities
25 that may be of assistance in carrying out the

1 purposes specified in subparagraphs (A) and
2 (B).

3 (7) PROTECTED SYSTEM.—The term “protected
4 system”—

5 (A) means any service, physical or com-
6 puter-based system, process, or procedure that
7 directly or indirectly affects a facility of critical
8 infrastructure; and

9 (B) includes any physical or computer-
10 based system, including a computer, computer
11 system, computer or communications network,
12 or any component hardware or element thereof,
13 software program, processing instructions, or
14 information or data in transmission or storage
15 therein, irrespective of the medium of trans-
16 mission or storage.

17 (8) VOLUNTARY.—

18 (A) IN GENERAL.—The term “voluntary”,
19 in the case of any submittal of critical infra-
20 structure information to a covered Federal
21 agency, means the submittal thereof in the ab-
22 sence of such agency’s exercise of legal author-
23 ity to compel access to or submission of such
24 information and may be accomplished by a sin-
25 gle entity or an Information Sharing and Anal-

1 ysis Organization on behalf of itself or its mem-
2 bers.

3 (B) EXCLUSIONS.—The term
4 “voluntary”—

5 (i) in the case of any action brought
6 under the securities laws as is defined in
7 section 3(a)(47) of the Securities Ex-
8 change Act of 1934 (15 U.S.C.
9 78c(a)(47))—

10 (I) does not include information
11 or statements contained in any docu-
12 ments or materials filed with the Se-
13 curities and Exchange Commission, or
14 with Federal banking regulators, pur-
15 suant to section 12(i) of the Securities
16 Exchange Act of 1934 (15 U.S.C.
17 781(I)); and

18 (II) with respect to the submittal
19 of critical infrastructure information,
20 does not include any disclosure or
21 writing that when made accompanied
22 the solicitation of an offer or a sale of
23 securities; and

1 (ii) does not include information or
2 statements required as a basis for making
3 licensing or permitting determinations.

4 **SEC. ___ 05. PROTECTION OF VOLUNTARILY SHARED CRIT-**
5 **ICAL INFRASTRUCTURE INFORMATION.**

6 (a) PROTECTION.—

7 (1) IN GENERAL.—Notwithstanding any other
8 provision of law, critical infrastructure information
9 (including the identity of the submitting person or
10 entity) that is voluntarily submitted to a covered
11 Federal agency for analysis, warning, interdepend-
12 ency study, recovery, reconstitution, or other infor-
13 mational purpose, when accompanied by an express
14 statement specified in paragraph (2)—

15 (A) shall be exempt from disclosure under
16 section 552 of title 5, United States Code (com-
17 monly referred to as the Freedom of Informa-
18 tion Act);

19 (B) shall not be subject to any agency
20 rules regarding ex parte communications with a
21 decision making official;

22 (C) shall not, without the written consent
23 of the person or entity submitting such infor-
24 mation, be used directly by such agency, any
25 other Federal, State, or local authority, or any

1 third party, in any civil action arising under
2 Federal or State law if such information is sub-
3 mitted in good faith; and

4 (D) shall not, without the written consent
5 of the person or entity submitting such infor-
6 mation, be used or disclosed for purposes other
7 than the purposes of this title, except—

8 (i) pursuant to the proper perform-
9 ance of the official duties of an officer or
10 employee of the United States; or

11 (ii) in furtherance of an investigation
12 or prosecution of a criminal act.

13 (2) EXPRESS STATEMENT.—For purposes of
14 paragraph (1), the term “express statement”, with
15 respect to information or records, means—

16 (A) in the case of written information or
17 records, a written marking on the information
18 or records substantially similar to the following:
19 “This information is voluntarily submitted to
20 the Federal Government in expectation of pro-
21 tection from disclosure as provided by the provi-
22 sions of the Critical Infrastructure Information
23 Act of 2001.”; or

24 (B) in the case of oral information, a simi-
25 lar statement that conveys that the information

1 is voluntarily submitted to the Government in
2 expectation of protection from disclosure, as is
3 provided by the provisions of this title.

4 (b) INDEPENDENTLY OBTAINED INFORMATION.—
5 Nothing in this section shall be construed to limit or other-
6 wise affect the ability of a State, local, or Federal Govern-
7 ment entity, agency, or authority, or any third party under
8 applicable law to obtain critical infrastructure information
9 in a manner not covered by subsection (a), including any
10 information lawfully and properly disclosed generally or
11 broadly to the public, and to use such information appro-
12 priately.

13 (c) TREATMENT OF VOLUNTARY SUBMITTAL OF IN-
14 FORMATION.—The voluntary submittal to the Government
15 of information or records that are protected from disclo-
16 sure by this title shall not be construed to constitute com-
17 pliance with any requirement to submit such information
18 to a Federal agency under any other provision of law.

19 (d) PROCEDURES.—

20 (1) IN GENERAL.—The Director of the Office of
21 Management and Budget shall, in consultation with
22 appropriate representatives of the National Security
23 Council and the Office of Science and Technology
24 Policy, establish uniform procedures for the receipt,
25 care, and storage by Federal agencies of critical in-

1 infrastructure information that is voluntarily sub-
2 mitted to the Government. The procedures shall be
3 established not later than 90 days after the date of
4 the enactment of this Act.

5 (2) ELEMENTS.—The procedures established
6 under paragraph (1) shall include mechanisms
7 regarding—

8 (A) the acknowledgement of receipt by
9 Federal agencies of critical infrastructure infor-
10 mation that is voluntarily submitted to the Gov-
11 ernment;

12 (B) the marking of such information as
13 voluntarily submitted to the Government for
14 purposes of this title;

15 (C) the care and storage of such informa-
16 tion; and

17 (D) the protection and maintenance of the
18 confidentiality of such information so as to per-
19 mit, pursuant to section ____06, the sharing of
20 such information within the Government, and
21 the issuance of notices and warnings related to
22 protection of critical infrastructure and pro-
23 tected systems, in such manner as to protect
24 from public disclosure the identity of the sub-
25 mitting person or entity, or information that is

1 proprietary, business sensitive, relates specifi-
2 cally to the submitting person or entity, or is
3 otherwise not appropriately in the public do-
4 main.

5 **SEC. ____06. NOTIFICATION, DISSEMINATION, AND ANAL-**
6 **YSIS REGARDING CRITICAL INFRASTRUC-**
7 **TURE INFORMATION.**

8 (a) NOTIFICATION REGARDING CRITICAL INFRA-
9 STRUCTURE SECURITY.—

10 (1) IN GENERAL.—A covered Federal agency
11 receiving significant and credible information under
12 section ____05 from a private person or entity about
13 the security of a protected system or critical infra-
14 structure of another known or identified private per-
15 son or entity shall notify and convey such informa-
16 tion to such other private person or entity as soon
17 as reasonable after receipt of such information by
18 the agency, to the extent consistent with—

19 (A) requirements of national security or
20 law enforcement; and

21 (B) the protection from public disclosure of
22 the identity of the submitting person or entity,
23 or information that is proprietary, business sen-
24 sitive, relates specifically to the submitting per-

1 son or entity, or is otherwise not appropriately
2 in the public domain.

3 (2) CONSTRUCTION.—

4 (A) Paragraph (1) shall not be construed
5 to require a covered Federal agency to provide
6 specific notice where doing so would not be
7 practicable, for example, based on the quantity
8 of persons or entities identified as having secu-
9 rity vulnerabilities. In instances where specific
10 notice is not practicable, the agency should take
11 reasonable steps, consistent with paragraph (1),
12 to issue broadly disseminated advisories or
13 alerts.

14 (B) Paragraph (1) shall not be construed
15 to require an agency to notify a third party if
16 the Government has reasonable grounds to be-
17 lieve that such party has conducted, or may be
18 conducting economic espionage against United
19 States entities within the meaning of the Eco-
20 nomic Espionage Act (18 U.S.C. 1831 et seq.),
21 if such person or entity derives support from
22 any nation currently under a trade embargo, or
23 if such person or entity has been identified,
24 pursuant to law, as a terrorist or terrorist enti-
25 ty.

1 (b) ANALYSIS OF INFORMATION.—Upon receipt of
2 critical infrastructure information that is voluntarily sub-
3 mitted to a covered Federal agency—

4 (1) the agency receiving such information shall
5 share with appropriate covered Federal agencies all
6 such information that concerns actual attacks, and
7 threats and warnings of attacks, on critical infra-
8 structure and protected systems;

9 (2) the Government shall identify interdepend-
10 encies; and

11 (3) the Government shall determine whether
12 further analysis, or warnings under subsection (c),
13 are warranted.

14 (c) ACTION FOLLOWING ANALYSIS.—

15 (1) AUTHORITY TO ISSUE WARNINGS.—As a re-
16 sult of analysis of critical infrastructure information
17 under subsection (b), a Federal agency may issue
18 advisories, alerts, and warnings to individual compa-
19 nies, targeted sectors, other governmental entities,
20 or the general public regarding potential threats to
21 critical infrastructure or protected systems.

22 (2) FORM OF WARNINGS.—In issuing a warning
23 under paragraph (1), the Federal agency concerned
24 shall take appropriate actions to protect from
25 disclosure—

1 (A) the source of any voluntarily submitted
2 critical infrastructure information that forms
3 the basis for the warning; or

4 (B) information that is proprietary, busi-
5 ness sensitive, relates specifically to the submit-
6 ting person or entity, or is otherwise not appro-
7 priately in the public domain.

8 (d) STRATEGIC ANALYSES OF POTENTIAL THREATS
9 TO CRITICAL INFRASTRUCTURE OR PROTECTED SYS-
10 TEMS.—

11 (1) IN GENERAL.—The President shall des-
12 ignate an element in the Executive Branch—

13 (A) to conduct strategic analyses of poten-
14 tial threats to critical infrastructure; and

15 (B) to submit reports on such analyses to
16 Information Sharing and Analysis Organiza-
17 tions and such other entities as the President
18 considers to be appropriate.

19 (2) STRATEGIC ANALYSES.—

20 (A) INFORMATION USED.—In conducting
21 strategic analyses under paragraph (1)(A), the
22 element designated to conduct such analyses
23 under paragraph (1) shall use a range of crit-
24 ical infrastructure information voluntarily sub-
25 mitted to the Government by the private sector,

1 as well as applicable intelligence and law en-
2 forcement information.

3 (B) AVAILABILITY.—The President shall
4 take appropriate actions to ensure that, to the
5 maximum extent practicable, all critical infra-
6 structure information voluntarily submitted to
7 the Government by the private sector is avail-
8 able to the element designated under paragraph
9 (1) to conduct strategic analyses under para-
10 graph (1)(A).

11 (C) FREQUENCY.—Strategic analyses shall
12 be conducted under this paragraph with such
13 frequency as the President considers to be ap-
14 propriate, and otherwise specifically at the di-
15 rection of the President.

16 (3) REPORTS.—

17 (A) IN GENERAL.—Each report under
18 paragraph (1)(B) shall contain the following:

19 (i) A description of currently recog-
20 nized methods of attacks on critical infra-
21 structure and protected systems.

22 (ii) An assessment of the threats to
23 critical infrastructure and protected sys-
24 tems that could develop over the year fol-
25 lowing such report.

1 (iii) An assessment of the lessons
2 learned from responses to previous attacks
3 on critical infrastructure and protected
4 systems.

5 (iv) Such other information on the
6 protection of critical infrastructure and
7 protected systems as the element con-
8 ducting analyses under paragraph (1) con-
9 siders appropriate.

10 (B) FORM.—Reports under paragraph
11 (1)(B) may be in classified or unclassified form,
12 or both, and shall be in such form as will pro-
13 tect from public disclosure—

14 (i) the source of any voluntarily sub-
15 mitted critical infrastructure information
16 that forms the basis for the warning; or

17 (ii) information that is proprietary,
18 business sensitive, relates specifically to
19 the submitting person or entity, or is oth-
20 erwise not appropriately in the public do-
21 main.

22 (4) CONSTRUCTION.—Nothing in this sub-
23 section shall be construed to modify or alter any re-
24 sponsibility of a Federal agency under subsections
25 (a), (b), and (c).

1 (e) PLAN FOR STRATEGIC ANALYSES OF THREATS
2 TO CRITICAL INFRASTRUCTURE AND PROTECTED SYS-
3 TEMS.—

4 (1) PLAN.—The President shall develop a plan
5 for carrying out strategic analyses of threats to crit-
6 ical infrastructure and protected systems through
7 the element in the Executive Branch designated
8 under subsection (d)(1).

9 (2) ELEMENTS.—The plan under paragraph (1)
10 shall include the following:

11 (A) A methodology for the work under the
12 plan of the element referred to in paragraph
13 (1), including the development of expertise
14 among the personnel of the element charged
15 with carrying out the plan and the acquisition
16 by the element of information relevant to the
17 plan.

18 (B) Mechanisms for the studying of
19 threats to critical infrastructure and protected
20 systems, and the issuance of warnings and rec-
21 ommendations regarding such threats, including
22 the allocation of personnel and other resources
23 of the element in order to carry out those mech-
24 anisms.

1 (C) An allocation of roles and responsibil-
2 ities for the work under the plan among the
3 covered Federal agencies, including the inter-
4 relationships among such roles and responsibil-
5 ities.

6 (3) REPORTS.—

7 (A) INTERIM REPORT.—The President
8 shall submit to Congress an interim report on
9 the plan developed under paragraph (1) not
10 later than 120 days after the date of the enact-
11 ment of this Act.

12 (B) FINAL REPORT.—The President shall
13 submit to Congress a final report on the plan
14 developed under paragraph (1), together with a
15 copy of the plan, not later than 180 days after
16 the date of the enactment of this Act.

17 **SEC. ___07. ANTITRUST EXEMPTION FOR ACTIVITY IN-**
18 **VOLVING AGREEMENTS ON CRITICAL INFRA-**
19 **STRUCTURE MATTERS.**

20 (a) ANTITRUST EXEMPTION.—Except as provided in
21 subsection (b), the antitrust laws shall not apply to con-
22 duct engaged in by an Information Sharing and Analysis
23 Organization or its members, including making and imple-
24 menting an agreement, solely for purposes of—

1 (1) gathering and analyzing critical infrastruc-
2 ture information in order to better understand secu-
3 rity problems related to critical infrastructure and
4 protected systems, and interdependencies of critical
5 infrastructure and protected systems, in order to en-
6 sure the availability, integrity, and reliability of crit-
7 ical infrastructure and protected systems;

8 (2) communicating or disclosing critical infra-
9 structure information to help prevent, detect, miti-
10 gate, or recover from the effects of a problem related
11 to critical infrastructure or protected systems; or

12 (3) voluntarily disseminating critical infrastruc-
13 ture information to its members, other Information
14 Sharing and Analysis Organizations, State, local, or
15 Federal Governments, or any entities that may be of
16 assistance in carrying out the purposes specified in
17 paragraphs (1) and (2).

18 (b) EXCEPTION.—Subsection (a) shall not apply with
19 respect to conduct that involves or results in an agreement
20 to boycott any person, to allocate a market, or to fix prices
21 or output.

22 **SEC. ____08. NO PRIVATE RIGHT OF ACTION.**

23 Nothing in this title may be construed to create a
24 private right of action for enforcement of any provision
25 of this title.