

107TH CONGRESS
1ST SESSION

S. 1456

To facilitate the security of the critical infrastructure of the United States, to encourage the secure disclosure and protected exchange of critical infrastructure information, to enhance the analysis, prevention, and detection of attacks on critical infrastructure, to enhance the recovery from such attacks, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 24, 2001

Mr. BENNETT (for himself and Mr. KYL) introduced the following bill; which was read twice and referred to the Committee on Governmental Affairs

A BILL

To facilitate the security of the critical infrastructure of the United States, to encourage the secure disclosure and protected exchange of critical infrastructure information, to enhance the analysis, prevention, and detection of attacks on critical infrastructure, to enhance the recovery from such attacks, and for other purposes.

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 “Critical Infrastructure
5 Information Security Act of 2001”.

1 **SEC. 2. FINDINGS.**

2 Congress makes the following findings:

3 (1) The critical infrastructures that underpin
4 our society, national defense, economic prosperity,
5 and quality of life—including energy, banking and
6 finance, transportation, vital human services, and
7 telecommunications—must be viewed in a new con-
8 text in the Information Age.

9 (2) The rapid proliferation and integration of
10 telecommunications and computer systems have con-
11 nected infrastructures to one another in a complex
12 global network of interconnectivity and interdepend-
13 ence. As a result, new vulnerabilities to such systems
14 and infrastructures have emerged, such as the threat
15 of physical and cyber attacks from terrorists or hos-
16 tile states. These attacks could disrupt the economy
17 and endanger the security of the United States.

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

1 (4) The private sector is hesitant to share crit-
2 ical infrastructure information with the Federal Gov-
3 ernment because—

4 (A) Federal law provides no clear assur-
5 ance that critical infrastructure information vol-
6 untarily submitted to the Federal Government
7 will be protected from disclosure or misuse;

8 (B) the framework of the Federal Govern-
9 ment for critical infrastructure information
10 sharing and analysis is not sufficiently devel-
11 oped; and

12 (C) concerns about possible prosecution
13 under the antitrust laws inhibit some companies
14 from partnering with other industry members,
15 including competitors, to develop cooperative in-
16 frastructure security strategies.

17 (5) Statutory nondisclosure provisions that
18 qualify as Exemption 3 statutes under section 552
19 of title 5, United States Code (commonly referred to
20 as the Freedom of Information Act), many of them
21 longstanding, prohibit disclosure of numerous classes
22 of information under that Act. These statutes cover
23 specific and narrowly defined classes of information
24 and are consistent with the principles of free and
25 open government that that Act seeks to facilitate.

1 (6) Since the infrastructure information that
2 this Act covers is not normally in the public domain,
3 preventing public disclosure of this sensitive infor-
4 mation serves the greater good by promoting na-
5 tional security and economic stability.

6 **SEC. 3. PURPOSE.**

7 The purpose of this Act is to foster improved security
8 of critical infrastructure by—

9 (1) promoting the increased sharing of critical
10 infrastructure information both between private sec-
11 tor entities and between the Federal Government
12 and the private sector; and

13 (2) encouraging the private sector and the Fed-
14 eral Government to conduct better analysis of crit-
15 ical infrastructure information in order to prevent,
16 detect, warn of, and respond to incidents involving
17 critical infrastructure.

18 **SEC. 4. DEFINITIONS.**

19 In this Act:

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

23 (2) CRITICAL INFRASTRUCTURE.—The term
24 “critical infrastructure”—

1 (A) means physical and cyber-based sys-
2 tems and services essential to the national de-
3 fense, government, or economy of the United
4 States, including systems essential for tele-
5 communications (including voice and data
6 transmission and the Internet), electrical power,
7 gas and oil storage and transportation, banking
8 and finance, transportation, water supply,
9 emergency services (including medical, fire, and
10 police services), and the continuity of govern-
11 ment operations; and

12 (B) includes any industry sector des-
13 ignated by the President pursuant to the Na-
14 tional Security Act of 1947 (50 U.S.C. 401 et
15 seq.) or the Defense Production Act of 1950
16 (50 U.S.C. App. 2061 et seq.) as essential to
17 provide resources for the execution of the na-
18 tional security strategy of the United States, in-
19 cluding emergency preparedness activities pur-
20 suant to title VI of the Robert T. Stafford Dis-
21 aster Relief and Emergency Assistance Act (42
22 U.S.C. 5195 et seq.).

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

1 (A) the ability of any protected system or
2 critical infrastructure to resist interference,
3 compromise, or incapacitation by either physical
4 or computer-based attack or other similar con-
5 duct that violates Federal, State, or local law,
6 harms interstate commerce of the United
7 States, or threatens public health or safety;

8 (B) any planned or past assessment, pro-
9 jection, or estimate of the security vulnerability
10 of a protected system or critical infrastructure,
11 including security testing, risk evaluation, risk
12 management planning, or risk audit;

13 (C) any planned or past operational prob-
14 lem or solution, including repair, recovery, re-
15 construction, insurance, or continuity, related to
16 the security of a protected system or critical in-
17 frastructure; or

18 (D) any threat to the security of a pro-
19 tected system or critical infrastructure.

20 (4) INFORMATION SHARING AND ANALYSIS OR-
21 GANIZATION.—The term “Information Sharing and
22 Analysis Organization” means any formal or infor-
23 mal entity or collaboration created by public or pri-
24 vate sector organizations, and composed primarily of
25 such organizations, for purposes of—

1 (A) gathering and analyzing critical infra-
2 structure information in order to better under-
3 stand security problems related to critical infra-
4 structure and protected systems, and inter-
5 dependencies of critical infrastructure and pro-
6 tected systems, so as to ensure the availability,
7 integrity, and reliability of critical infrastruc-
8 ture and protected systems;

9 (B) communicating or disclosing critical
10 infrastructure information to help prevent, de-
11 tect, mitigate, or recover from the effects of a
12 problem related to critical infrastructure or pro-
13 tected systems; and

14 (C) voluntarily disseminating critical infra-
15 structure information to entity members, other
16 Information Sharing and Analysis Organiza-
17 tions, the Federal Government, or any entities
18 which may be of assistance in carrying out the
19 purposes specified in subparagraphs (A) and
20 (B).

21 (5) PROTECTED SYSTEM.—The term “protected
22 system”—

23 (A) means any service, physical or com-
24 puter-based system, process, or procedure that

1 directly or indirectly affects a facility of critical
2 infrastructure; and

3 (B) includes any physical or computer-
4 based system, including a computer, computer
5 system, computer or communications network,
6 or any component hardware or element thereof,
7 software program, processing instructions, or
8 information or data in transmission or storage
9 therein (irrespective of storage medium).

10 (6) VOLUNTARY.—The term “voluntary”, in the
11 case of the submittal of information or records to
12 the Federal Government, means the submittal of the
13 information or records in the absence of an agency’s
14 exercise of legal submission.

15 **SEC. 5. PROTECTION OF VOLUNTARILY SHARED CRITICAL**
16 **INFRASTRUCTURE INFORMATION.**

17 (a) PROTECTION.—

18 (1) IN GENERAL.—Notwithstanding any other
19 provision of law, critical infrastructure information
20 that is voluntarily submitted to a covered Federal
21 agency for analysis, warning, interdependency study,
22 recovery, reconstitution, or other informational pur-
23 pose, when accompanied by an express statement
24 specified in paragraph (3)—

1 (A) shall not be made available under sec-
2 tion 552 of title 5, United States Code (com-
3 monly referred to as the Freedom of Informa-
4 tion Act);

5 (B) may not, without the written consent
6 of the person or entity submitting such infor-
7 mation, be used directly by such agency, any
8 other Federal, State, or local authority, or any
9 third party, in any civil action arising under
10 Federal or State law, unless such information is
11 submitted in bad faith; and

12 (C) may not, without the written consent
13 of the person or entity submitting such infor-
14 mation, be used for a purpose other than the
15 purpose of this Act, or disclosed by any officer
16 or employee of the United States, except pursu-
17 ant to the official duties of such officer or em-
18 ployee pursuant to this Act.

19 (2) COVERED FEDERAL AGENCY DEFINED.—In
20 paragraph (1), the term “covered Federal agency”
21 means the following:

22 (A) The Department of Justice.

23 (B) The Department of Defense.

24 (C) The Department of Commerce.

25 (D) The Department of Transportation.

1 (E) The Department of the Treasury.

2 (F) The Department of Health and
3 Human Services.

4 (G) The Department of Energy.

5 (H) The Environmental Protection Agency.

6 (I) The General Services Administration.

7 (J) The Federal Communications Commis-
8 sion.

9 (K) The Federal Emergency Management
10 Agency.

11 (L) The National Infrastructure Protection
12 Center.

13 (M) The National Communication System.

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

17 (A) in the case of written information or
18 records, a written marking on the information
19 or records as follows: “This information is vol-
20 untarily submitted to the Federal Government
21 in expectation of protection from disclosure
22 under the provisions of the Critical Infrastruc-
23 ture Information Security Act of 2001.”; or

24 (B) in the case of oral information, a
25 statement, substantially similar to the words

1 specified in subparagraph (A), to convey that
2 the information is voluntarily submitted to the
3 Federal Government in expectation of protec-
4 tion from disclosure under the provisions of this
5 Act.

6 (b) INDEPENDENTLY OBTAINED INFORMATION.—
7 Nothing in this section shall be construed to limit or other-
8 wise affect the ability of the Federal Government to obtain
9 and use under applicable law critical infrastructure infor-
10 mation obtained by or submitted to the Federal Govern-
11 ment in a manner not covered by subsection (a).

12 (c) TREATMENT OF VOLUNTARY SUBMITTAL OF IN-
13 FORMATION.—The voluntary submittal to the Federal
14 Government of information or records that are protected
15 from disclosure by this section shall not be construed to
16 constitute compliance with any requirement to submit
17 such information to a Federal agency under any other pro-
18 vision 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 Federal Government. The procedures
3 shall be established not later than 90 days after the
4 date of 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 Fed-
11 eral Government, including confirmation that
12 such information is protected from disclosure
13 under this Act;

14 (B) the marking of such information as
15 critical infrastructure information that is volun-
16 tarily submitted to the Federal Government for
17 purposes of this Act;

18 (C) the care and storage of such informa-
19 tion; and

20 (D) the protection and maintenance of the
21 confidentiality of such information so as to per-
22 mit, pursuant to section 6, the sharing of such
23 information within the Federal Government,
24 and the issuance of notices and warnings re-
25 lated to protection of critical infrastructure.

1 **SEC. 6. NOTIFICATION, DISSEMINATION, AND ANALYSIS RE-**
2 **GARDING CRITICAL INFRASTRUCTURE IN-**
3 **FORMATION.**

4 (a) NOTICE REGARDING CRITICAL INFRASTRUCTURE
5 SECURITY.—

6 (1) IN GENERAL.—A covered Federal agency
7 (as specified in section 5(a)(2)) receiving significant
8 and credible information under section 5 from a pri-
9 vate person or entity about the security of a pro-
10 tected system or critical infrastructure of another
11 known or identified private person or entity shall, to
12 the extent consistent with requirements of national
13 security or law enforcement, notify and convey such
14 information to such other private person or entity as
15 soon as reasonable after receipt of such information
16 by the agency.

17 (2) CONSTRUCTION.—Paragraph (1) may not
18 be construed to require an agency to provide specific
19 notice where doing so would not be practicable, for
20 example, based on the quantity of persons or entities
21 identified as having security vulnerabilities. In in-
22 stances where specific notice is not practicable, the
23 agency should take reasonable steps, consistent with
24 paragraph (1), to issue broadly disseminated
25 advisories or alerts.

1 (b) ANALYSIS OF INFORMATION.—Upon receipt of
2 critical infrastructure information that is voluntarily sub-
3 mitted to the Federal Government, the Federal agency re-
4 ceiving such information shall—

5 (1) share with appropriate covered Federal
6 agencies (as so specified) all such information that
7 concerns actual attacks, and threats and warnings of
8 attacks, on critical infrastructure and protected sys-
9 tems;

10 (2) identify interdependencies; and

11 (3) determine whether further analysis in con-
12 cert with other Federal agencies, or warnings under
13 subsection (c), 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 warnings to individual companies, targeted sectors,
19 other governmental entities, or the general public re-
20 garding potential threats to critical infrastructure.

21 (2) FORM OF WARNINGS.—In issuing a warning
22 under paragraph (1), the Federal agency concerned
23 shall take appropriate actions to prevent the disclo-
24 sure of the source of any voluntarily submitted crit-

1 ical infrastructure information that forms the basis
2 for the warning.

3 (d) STRATEGIC ANALYSES OF POTENTIAL THREATS
4 TO CRITICAL INFRASTRUCTURE.—

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

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

9 (B) to submit reports on such analyses to
10 Information Sharing and Analysis Organiza-
11 tions and such other entities as the President
12 considers appropriate.

13 (2) STRATEGIC ANALYSES.—

14 (A) INFORMATION USED.—In conducting
15 strategic analyses under paragraph (1)(A), the
16 element designated to conduct such analyses
17 under paragraph (1) shall utilize a range of
18 critical infrastructure information voluntarily
19 submitted to the Federal Government by the
20 private sector, as well as applicable intelligence
21 and law enforcement information.

22 (B) AVAILABILITY.—The President shall
23 take appropriate actions to ensure that, to the
24 maximum extent practicable, all critical infra-
25 structure information voluntarily submitted to

1 the Federal Government by the private sector is
2 available to the element designated under para-
3 graph (1) to conduct strategic analyses under
4 paragraph (1)(A).

5 (C) FREQUENCY.—Strategic analyses shall
6 be conducted under this paragraph with such
7 frequency as the President considers appro-
8 priate, and otherwise specifically at the direc-
9 tion of the President.

10 (3) REPORTS.—

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

13 (i) A description of currently recog-
14 nized methods of attacks on critical infra-
15 structure.

16 (ii) An assessment of the threats to
17 critical infrastructure that could develop
18 over the year following such report.

19 (iii) An assessment of the lessons
20 learned from responses to previous attacks
21 on critical infrastructure.

22 (iv) Such other information on the
23 protection of critical infrastructure as the
24 element conducting analyses under para-
25 graph (1) considers appropriate.

1 (B) FORM.—Reports under this paragraph
2 may be in classified or unclassified form, or
3 both.

4 (4) CONSTRUCTION.—Nothing in this sub-
5 section shall be construed to modify or alter any re-
6 sponsibility of a Federal agency under subsections
7 (a) through (e).

8 (e) PLAN FOR STRATEGIC ANALYSES OF THREATS
9 TO CRITICAL INFRASTRUCTURE.—

10 (1) PLAN.—The President shall develop a plan
11 for carrying out strategic analyses of threats to crit-
12 ical infrastructure through the element in the Exec-
13 utive Branch designated under subsection (d)(1).

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

16 (A) A methodology for the work under the
17 plan of the element referred to in paragraph
18 (1), including the development of expertise
19 among the personnel of the element charged
20 with carrying out the plan and the acquisition
21 by the element of information relevant to the
22 plan.

23 (B) Mechanisms for the studying of
24 threats to critical infrastructure, and the
25 issuance of warnings and recommendations re-

1 garding such threats, including the allocation of
2 personnel and other resources of the element in
3 order to carry out those mechanisms.

4 (C) An allocation of roles and responsibil-
5 ities for the work under the plan among the
6 Federal agencies specified in section 5(a)(2), in-
7 cluding the relationship of such roles and re-
8 sponsibilities.

9 (3) REPORTS.—

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

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

20 **SEC. 7. ANTITRUST EXEMPTION FOR ACTIVITY INVOLVING**
21 **AGREEMENTS ON CRITICAL INFRASTRUC-**
22 **TURE MATTERS.**

23 (a) ANTITRUST EXEMPTION.—The antitrust laws
24 shall not apply to conduct engaged in by an Information
25 Sharing and Analysis Organization or its members, includ-

1 ing making and implementing an agreement, solely for
2 purposes of—

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

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

14 (3) voluntarily disseminating critical infrastruc-
15 ture information to entity members, other Informa-
16 tion Sharing and Analysis Organizations, the Fed-
17 eral Government, or any entities which may be of as-
18 sistance in carrying out the purposes specified in
19 paragraphs (1) and (2).

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

24 (c) ANTITRUST LAWS DEFINED.—In this section, the
25 term “antitrust laws”—

1 (1) has the meaning given such term in sub-
2 section (a) of the first section of the Clayton Act (15
3 U.S.C. 12(a)), except that such term includes sec-
4 tion 5 of the Federal Trade Commission Act (15
5 U.S.C. 45) to the extent such section 5 applies to
6 unfair methods of competition; and

7 (2) includes any State law similar to the laws
8 referred to in paragraph (1).

9 **SEC. 8. NO PRIVATE RIGHT OF ACTION.**

10 Nothing in this Act may be construed to create a pri-
11 vate right of action for enforcement of any provision of
12 this Act.

○