

106TH CONGRESS
2D SESSION

S. 3188

To facilitate the protection of the critical infrastructure of the United States, to enhance the investigation and prosecution of computer-related crimes, and for other purposes.

IN THE SENATE OF THE UNITED STATES

OCTOBER 11 (legislative day, SEPTEMBER 22), 2000

Mr. KYL (for himself and Mrs. FEINSTEIN) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

A BILL

To facilitate the protection of the critical infrastructure of the United States, to enhance the investigation and prosecution of computer-related crimes, 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 “Cyber Security En-
5 hancement Act”.

6 **SEC. 2. FINDINGS.**

7 Congress makes the following findings:

1 (1) The ability of the Federal Government to
2 obtain information on threats and risks to the crit-
3 ical infrastructure of the United States, whether op-
4 erated by the public sector or private sector and
5 whether domestic or foreign, is vital to the mainte-
6 nance of United States security and the economic
7 well-being of the United States.

8 (2) Persons in the private sector and non-Fed-
9 eral governmental agencies have expressed a willing-
10 ness to voluntarily provide sensitive information on
11 critical infrastructure threats and vulnerabilities to
12 the Federal Government contingent on the ability of
13 the Federal Government to protect such information
14 from unrestricted disclosure.

15 (3) The Federal Government needs critical in-
16 frastructure information from persons in the private
17 sector and non-Federal governmental agencies in
18 order to protect critical infrastructure from inten-
19 tional acts of significant harm.

20 (4) The public interest is best served by pre-
21 serving the confidentiality of critical infrastructure
22 information that is submitted to the Federal Govern-
23 ment to the extent necessary to encourage the sub-
24 mittal of such information to the Federal Govern-
25 ment.

1 (5) Current Federal law does not provide per-
2 sons in the private sector and non-Federal govern-
3 mental agencies with clear assurance that informa-
4 tion submitted to the Federal Government on
5 threats and risks to critical infrastructure will be
6 protected from disclosure under section 552 of title
7 5, United States Code (commonly referred to as the
8 Freedom of Information Act).

9 (6) There are currently more than 100 exemp-
10 tions from disclosure of information under the Free-
11 dom of Information Act that have been approved by
12 law for other purposes.

13 (7) President Clinton has acknowledged the na-
14 tional security issues that result from the cyber
15 vulnerabilities of the United States in stating that
16 “[w]e must be ready . . . ready if our adversaries
17 try to use computers to disable our power grids,
18 banking, communications and transportation net-
19 works, police, fire and health services, or military as-
20 sets”.

21 (8) Information sharing among private sector
22 organizations is critical to help identify
23 vulnerabilities and threats to information networks.
24 Many companies are wary of participating in cyber

1 security information sharing activities with one an-
2 other due to concerns about antitrust penalties.

3 (9) Currently, the maximum penalties for Fed-
4 eral computer crimes are inadequate to punish and
5 deter the most serious computer crimes.

6 (10) In order to catch cyber criminals, a cyber
7 attack must be swiftly traced to its source.

8 (11) A lack of standardization among law en-
9 forcement agencies has hindered effective informa-
10 tion gathering from industry during investigation of
11 cyber crimes.

12 (12) Many cyber attacks are complicated by the
13 criminal's use of a false Internet protocol (IP) ad-
14 dress, thus masking the origin of the attack. There
15 is no legitimate use for a false IP address.

16 **SEC. 3. LIMITATION ON DISCLOSURE OF CERTAIN SEN-**
17 **SITIVE INFORMATION UNDER THE FREEDOM**
18 **OF INFORMATION ACT.**

19 (a) **LIMITATION.**—Critical infrastructure informa-
20 tion, records relating to critical infrastructure informa-
21 tion, and information on critical infrastructure protection
22 derived from such information or records that is submitted
23 voluntarily by a non-Federal source to a critical infra-
24 structure protection office or program shall not be made
25 available under section 552 of title 5, United States Code

1 (commonly referred to as the Freedom of Information
2 Act), if the person submitting such information or records
3 expressly requests that such information or records, or in-
4 formation derived therefrom, not be made available under
5 that section.

6 (b) DESIGNATION OF OFFICE OR PROGRAM.—

7 (1) DESIGNATION.—The President or the head
8 of a Federal agency may designate an element in the
9 agency as a critical infrastructure office or program
10 for purposes of subsection (a). The head of an agen-
11 cy may not delegate the authority in the preceding
12 sentence.

13 (2) PUBLICATION OF NOTICE.—The head of the
14 Federal agency concerned shall publish in the Fed-
15 eral Register a notice of intent to designate an ele-
16 ment in the Federal agency as a critical infrastruc-
17 ture office or program not later than 30 days before
18 the effective date of such designation.

19 (c) REQUEST FOR PROTECTION.—

20 (1) IN GENERAL.—A person seeking the protec-
21 tion of information or records under subsection (a)
22 shall be treated as having made an express request
23 for protection under that subsection if the person
24 marks the information or records substantially as
25 follows: “ _____ is submitted to a critical in-

1 frastructure protection office or program under the
2 provisions of section 3(a) of the Cyber Security En-
3 hancement Act.” (the blank being filled in with in-
4 formation sufficient to identify the information or
5 records concerned).

6 (2) LIMITATION.—A request with respect to in-
7 formation or records under subsection (a) may be
8 made only by the person submitting such informa-
9 tion or records to the Federal Government.

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

16 (e) OPERATION OF STATE AND LOCAL LAW.—

17 (1) CONTROL OF UNITED STATES.—Informa-
18 tion or records protected from disclosure under sub-
19 section (a) shall be treated as under the control of
20 the Federal Government even if made available to a
21 State or local government.

22 (2) INAPPLICABILITY OF STATE OR LOCAL DIS-
23 CLOSURE LAW.—No State or local law requiring
24 public disclosure of information or records shall
25 apply to information or records obtained by the Fed-

1 eral Government that are protected from disclosure
2 under subsection (a).

3 (f) TREATMENT OF VOLUNTARY SUBMITTAL OF IN-
4 FORMATION.—The voluntary submission of information or
5 records that are protected from disclosure by this section
6 shall not be construed to constitute compliance with any
7 requirement to submit such information to a Federal
8 agency under any other provision of law.

9 (g) WITHDRAWAL OF REQUEST FOR PROTECTION.—

10 (1) WITHDRAWAL.—A request that information
11 or records be protected from disclosure under sub-
12 section (a) may be withdrawn at any time by the
13 person making the request.

14 (2) EFFECT.—The withdrawal of a request
15 under paragraph (1) shall take effect upon receipt of
16 the withdrawal by the Federal agency concerned.

17 (h) TIME LIMITATIONS ON PROTECTION.—

18 (1) IN GENERAL.—Subject to paragraph (2),
19 the protection of information or records under sub-
20 section (a) shall expire at the end of the five-year
21 period beginning on the date of submittal of such in-
22 formation or records to the Federal Government.

23 (2) EXTENSION.—Upon the expiration of the
24 protection of information or records under this sec-
25 tion, including any extension of such protection

1 under this subsection, such protection may be ex-
2 tended by an additional period of 5 years.

3 (3) PROCEDURE AFTER EXPIRATION.—After ex-
4 piration under this subsection of the period of pro-
5 tection of information or records under this section,
6 the Federal agency concerned shall, upon receipt of
7 a request for such information or records under sec-
8 tion 552 of title 5, United States Code, determine
9 whether the person who originally requested the pro-
10 tection of such information or records under this
11 section seeks to continue the protection of such in-
12 formation or records under this section. If such per-
13 son does not seek continuation of the protection of
14 such information or records under this section, the
15 protection of such information or records under this
16 section shall cease.

17 (i) PENALTIES FOR UNAUTHORIZED DISCLOSURE.—

18 (1) INVESTIGATION.—If a court finds that a
19 Federal agency has violated this section, and finds
20 that the circumstances of the violation raise ques-
21 tions whether or not an officer or employee of the
22 agency acted willfully or intentionally with respect to
23 the violation, the agency shall promptly investigate
24 whether or not disciplinary action is warranted
25 against the officer or employee.

1 (2) **AUTHORITY TO ACT.**—Appropriate discipli-
2 nary action may be imposed as a result of an inves-
3 tigation under paragraph (1).

4 (j) **SCOPE OF PROTECTION.**—This section may not
5 be construed to preclude a Federal agency from estab-
6 lishing procedures for sharing critical infrastructure pro-
7 tection information within and outside the Federal Gov-
8 ernment for purposes related to protecting critical infra-
9 structure.

10 **SEC. 4. ANTITRUST MATTERS.**

11 (a) **ANTITRUST EXEMPTION.**—Except as provided in
12 subsection (b), the antitrust laws shall not apply to con-
13 duct engaged in, including making and implementing an
14 agreement, solely for the purpose of and limited to—

15 (1) facilitating responses intended to correct or
16 avoid a cyber security related problem; or

17 (2) communicating or disclosing information to
18 help correct or avoid the effects of a cyber security
19 related problem.

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) **RULE OF CONSTRUCTION.**—The exemption grant-
25 ed by subsection (a) shall be construed narrowly.

1 **SEC. 5. FRAUD AND RELATED ACTIVITY IN CONNECTION**
 2 **WITH COMPUTERS.**

3 (a) ENHANCED PENALTIES.—Subsection (c) of that
 4 section is amended—

5 (1) in paragraph (2)(B), by striking “5 years”
 6 and inserting “10 years”;

7 (2) in paragraph (2)(C), by striking “ten
 8 years” and inserting “20 years”;

9 (3) in paragraph (3)(A), by striking “five
 10 years” and inserting “10 years”; and

11 (4) in paragraph (3)(B), by striking “ten
 12 years” and inserting “20 years”.

13 **SEC. 6. ADMINISTRATIVE SUBPOENAS IN CASES INVOLVING**
 14 **CYBER CRIME.**

15 (a) IN GENERAL.—Chapter 223 of title 18, United
 16 States Code, is amended by inserting after section 3486A
 17 the following new section:

18 **“§ 3486B. Administrative subpoenas in cases involv-**
 19 **ing cyber crime**

20 “(a) AUTHORIZATION.—

21 “(1) IN GENERAL.—In any investigation relat-
 22 ing to any act or activity involving a violation of sec-
 23 tion 871, 879, 1029, 1030, 1362, 2511, 2701, 2702,
 24 or 2703 of this title, the Attorney General, or the
 25 designee of the Attorney General, may issue in writ-
 26 ing and cause to be served a subpoena—

1 “(A) requiring a provider of electronic
2 communication service or remote computing
3 service to disclose the name, address, Internet
4 protocol address (IP address), local and long
5 distance telephone toll billing records, telephone
6 number or other subscriber number or identity,
7 and length of service of a subscriber to or cus-
8 tomer of such service and the types of services
9 the subscriber or customer utilized, which may
10 be relevant to an authorized law enforcement
11 inquiry; or

12 “(B) requiring a custodian of records to
13 give testimony concerning the production and
14 authentication of such records or information.

15 “(2) LIMITATION ON DISCLOSURE.—Informa-
16 tion disclosed under paragraph (1) may not include
17 content of an electronic communication.

18 “(3) ATTENDANCE OF WITNESSES.—Witnesses
19 summoned under this section shall be paid the same
20 fees and mileage that are paid witnesses in the
21 courts of the United States.

22 “(b) PROCEDURES APPLICABLE.—The same proce-
23 dures for service and enforcement as are provided with
24 respect to investigative demands under section 3486 of

1 this title shall apply with respect to a subpoena issued
2 under this section.”.

3 (b) CLERICAL AMENDMENT.—The table of sections
4 at the beginning of chapter 223 of such title is amended
5 by inserting after the item relating to section 3486A the
6 following new item:

“3486B. Administrative subpoenas in cases involving cyber crime.”.

7 **SEC. 7. STANDARDIZED REQUESTS FOR ELECTRONIC IN-**
8 **FORMATION AND RECORDS.**

9 (a) PLAN TO ENCOURAGE STANDARDIZED RE-
10 QUESTS.—Not later than six months after the date of the
11 enactment of this Act, the Attorney General shall submit
12 to the President and to the Committees on the Judiciary
13 of the Senate and House of Representatives a plan to en-
14 courage the standardization of requests of Federal, State,
15 and local law enforcement agencies to Internet service pro-
16 viders (ISPs) and other entities for electronic information
17 and records used in the investigation of computer fraud
18 and other computer-related crimes.

19 (b) CONSULTATION.—In preparing the plan, the At-
20 torney General shall consult with the heads of other appro-
21 priate Federal agencies, appropriate representatives of
22 State and local law enforcement agencies, and other inter-
23 ested persons.

1 (c) NOTICE AND COMMENT.—In preparing the plan,
2 the Attorney General shall seek public notice and comment
3 on the plan.

4 **SEC. 8. PREVENTION OF INTERNET PROTOCOL ADDRESS**
5 **SPOOFING.**

6 (a) PLAN TO ENCOURAGE PREVENTION.—Not later
7 than six months after the date of the enactment of this
8 Act, the Attorney General and the Secretary of Commerce
9 shall jointly submit to Congress and the President a plan
10 to encourage Internet service providers to take appropriate
11 actions to prevent or impede the use of false Internet pro-
12 tocol addresses as a means of access to Internet servers
13 (commonly referred to as “IP spoofing”), including the in-
14 stallation and use of Internet servers and routers, and so-
15 called “firewall” software, which prevent, impede, or oth-
16 erwise provide protection against the use of such addresses
17 for that purpose.

18 (b) CONSULTATION.—In preparing the plan, the At-
19 torney General and the Secretary of Commerce shall joint-
20 ly consult with the heads of other appropriate Federal
21 agencies, appropriate representatives of State and govern-
22 ments, and other interested persons.

23 (c) NOTICE AND COMMENT.—In preparing the plan,
24 the Attorney General and the Secretary of Commerce shall
25 seek public notice and comment on the plan.

1 **SEC. 9. DEFINITIONS.**

2 In this Act:

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

6 (2) ANTITRUST LAWS.—The term “antitrust
7 laws”—

8 (A) has the meaning given such term in
9 subsection (a) of the first section of the Clayton
10 Act (15 U.S.C. 12(a)), except that such term
11 includes section 5 of the Federal Trade Com-
12 mission Act (15 U.S.C. 45) to the extent such
13 section 5 applies to unfair methods of competi-
14 tion: and

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

17 (3) CRITICAL INFRASTRUCTURE.—The term
18 “critical infrastructure” means physical and cyber-
19 based systems, facilities, or services so essential to
20 the United States or the United States economy that
21 the disruption, incapacity, or destruction of such
22 systems, facilities, or services would have a debili-
23 tating impact on the defense, security, economic
24 prosperity, or health or safety of the United States.

25 (4) CRITICAL INFRASTRUCTURE INFORMA-
26 TION.—The term “critical infrastructure informa-

1 tion” means information concerning threats,
2 vulnerabilities, risks, and mitigation of same perti-
3 nent to critical infrastructure.

4 (5) CRITICAL INFRASTRUCTURE PROTECTION
5 OFFICE OR PROGRAM.—The term “critical infra-
6 structure protection office or program” means an
7 element of a Federal agency that is designated by
8 the President or the head of the agency as having
9 functions relating to the protection of critical infra-
10 structure from intentional acts or significant harm.

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

22 (7) VOLUNTARY.—The term “voluntary”, in the
23 case of submittal of information or records to the
24 Federal Government, means that the information or
25 records were submitted—

- 1 (A) without mandate or compulsion; and
- 2 (B) not as a condition of doing business
- 3 with the Federal Government.

○