107TH CONGRESS
1ST SESSION

S. _____

IN THE SENATE OF THE UNITED STATES

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

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, and for other purposes.

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 ''Critical Infrastructure Information Security Act of 2001''.

SEC. 2. FINDINGS.

Congress makes the following findings:

(1) The critical infrastructures that underpin our society, national defense, economic prosperity,

and quality of life—including energy, banking and finance, transportation, vital human services, and telecommunications—must be viewed in a new context in the Information Age.

(2) The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex global network of interconnectivity and interdependence. As a result, new vulnerabilities to such systems and infrastructures have emerged, such as the threat of physical and cyber attacks from terrorists or hostile states. These attacks could disrupt the economy and endanger the security of the United States.

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

(4) The private sector is hesitant to share critical infrastructure information with the Federal Government because—

(A) Federal law provides no clear assurance that critical infrastructure information

submitted to the Federal Government will be protected from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act);

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

(C) concerns about possible prosecution under the antitrust laws inhibit some companies from partnering with other industry members, including competitors, to develop cooperative infrastructure security strategies.

(5) Statutory exemptions to the Freedom of Information Act, many of them longstanding, designate nearly 100 classes of information as not subject to that Act. These classes of information are specific and very narrowly defined, consistent with the principles of free and open government that the Act seeks to facilitate.

(6) Since critical infrastructure information is not normally in the public domain, preventing public disclosure of this sensitive information serves the greater good by promoting national security and economic stability.

SEC. 3. PURPOSE.

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

(1) promoting the increased sharing of critical infrastructure information both between private sector entities and between the Federal Government and the private sector; and

(2) encouraging the private sector and the Federal Government to conduct better analysis of critical infrastructure information in order to prevent, detect, warn of, and respond to incidents involving critical infrastructure.

SEC. 4. DEFINITIONS.

In this Act:

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

(2) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure''—

(A) means any industry sector that provides a continual flow of goods and services essential to the defense or economic security of the United States, the functioning of government, or the health, welfare, or safety of the public; and

(B) includes any industry sector designated by the President pursuant to the National Security Act of 1947 (50 U.S.C. 401 et seq.), the Defense Production Act of 1950 (50 U.S.C. App. 2061 et seq.), or the Federal Civil Defense Act of 1950 (50 U.S.C. App. 2251 et seq.) as essential to provide resources for the execution of the national security strategy of the United States, including emergency preparedness.

(3) CRITICAL INFRASTRUCTURE INFORMATION.—The term ''critical infrastructure information'' means information related to—

(A) the ability of any protected system or critical infrastructure to resist intentional or unintentional interference, compromise, or incapacitation through the misuse of or unauthorized access to or use of the Internet, public or private telecommunication systems, or other similar conduct that violates Federal, State, local, or international law, harms interstate commerce of the United States, or threatens public health or safety;

(B) any planned or past assessment, projection, or estimate of the security vulnerability

of a protected system or critical infrastructure, including security testing, risk evaluation, risk management planning, or risk audit;

(C) any planned or past operational problem or solution, including repair, recovery, reconstruction, insurance, or continuity, related to the security of a protected system or critical infrastructure; or

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

(4) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term ''Information Sharing and Analysis Organization'' means any formal or informal entity or collaboration created by public or private sector organizations, and composed primarily of such organizations, for purposes of—

(A) gathering and analyzing critical infrastructure information in order to better understand security problems related to critical infrastructure and protected systems, and interdependencies of critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability of critical infrastructure and protected systems;

(B) communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a problem related to critical infrastructure or protected systems; and

(C) voluntarily disseminating critical infrastructure information to entity members, other Information Sharing and Analysis Organizations, the Federal Government, or any entities which may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

(5) PROTECTED SYSTEM.—The term ''protected system''—

(A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects a facility of critical infrastructure; and

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

(6) VOLUNTARY.—The term ''voluntary'', in the case of the submittal of information or records to the Federal Government, means the submittal of the information or records without mandate or compulsion, whether under statute, court decision, or regulation.

SEC. 5. PROTECTION OF VOLUNTARILY SHARED CRITICAL INFRASTRUCTURE INFORMATION.

(a) PROTECTION.—

(1) IN GENERAL.—Critical infrastructure information that is voluntarily submitted to a covered Federal agency for analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (3)—

(A) shall not be made available under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act); and

(B) may not, without the written consent of the person or entity submitting such information, be used by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law.

(2) COVERED FEDERAL AGENCY DEFINED.—In paragraph (1), the term ''covered Federal agency'' means the following:

(A) The Department of Justice.

(B) The Department of Defense.

(C) The Department of Commerce.

(D) The Department of Transportation.

(E) The Department of the Treasury.

(F) The Department of Health and Human Services.

(G) The Department of Energy.

(H) The Environmental Protection Agency.

(I) The General Services Administration.

(J) The Federal Communications Commission.

(K) The Federal Emergency Management Agency.

(L) The National Infrastructure Protection Center.

(M) The National Communication System.

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

(A) in the case of written information or records, a written marking on the information

or records as follows: ''This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure under the provisions of the Critical Infrastructure Information Security Act of 2001.''; or

(B) in the case of oral information, a statement, substantially similar to the words specified in subparagraph (A), to convey that the information is voluntarily submitted to the Federal Government in expectation of protection from disclosure under the provisions of this Act.

(b) INDEPENDENTLY OBTAINED INFORMATION.—Nothing in this section shall be construed to limit or otherwise affect the ability of the Federal Government to obtain and use under applicable law critical infrastructure information obtained by or submitted to the Federal Government in a manner not covered by subsection (a).

(c) OPERATION OF STATE AND LOCAL LAW.—

(1) CONTROL OF UNITED STATES.—Information or records protected from disclosure under subsection (a) shall be treated as under the control of the Federal Government even if also made available to a State or local government.

(2) INAPPLICABILITY OF STATE OR LOCAL DISCLOSURE LAW.—No State or local law requiring disclosure of information or records shall apply to any information or records protected from disclosure under subsection (a) that are provided to such State or local government by the Federal Government, or by an Information Sharing and Analysis Organization, for purposes for which such information or records would be protected from disclosure under that subsection.

(d) TREATMENT OF VOLUNTARY SUBMITTAL OF INFORMATION.—The voluntary submittal to the Federal Government of information or records that are protected from disclosure by this section shall not be construed to constitute compliance with any requirement to submit such information to a Federal agency under any other provision of law.

(e) PROCEDURES.—

(1) IN GENERAL.—The Director of the Office of Management and Budget shall require the Administrative Conference of the United States, in consultation with appropriate representatives of the National Security Council, to establish uniform procedures for the receipt, care, and storage by Federal agencies of critical infrastructure information that is voluntarily

submitted to the Federal Government. The procedures shall be established not later than 90 days after the date of the enactment of this Act.

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

(A) the acknowledgement of receipt by Federal agencies of critical infrastructure information that is voluntarily submitted to the Federal Government, including confirmation that such information is protected from disclosure under this Act;

(B) the marking of such information as critical infrastructure that is voluntarily submitted to the Federal Government for purposes of this Act;

(C) the care and storage of such information; and

(D) the protection and maintenance of the confidentiality of such information so as to permit, pursuant to section 6, the sharing of such information within the Federal Government, and the issuance of notices and warnings related to protection of critical infrastructure.

(f) BURDEN OF PROOF IN ACTIONS FOR PRODUCTION.—Notwithstanding section 552(a)(4)(B) of title 5, United States Code, or any other provision of law, in any action or proceeding to enjoin a Federal agency from withholding information or records under this section, or to compel the production of information or records protected from disclosure under this section, the burden shall be on the person seeking disclosure to demonstrate, by clear and convincing evidence, that the information or records whose production is sought is not protected from disclosure under this section.

SEC. 6. NOTIFICATION, DISSEMINATION, AND ANALYSIS REGARDING CRITICAL INFRASTRUCTURE INFORMATION.

(a) NOTICE REGARDING CRITICAL INFRASTRUCTURE SECURITY.—

(1) IN GENERAL.—A Federal agency or other Federal authority receiving significant and credible information from a private person or entity about the security of a protected system or critical infrastructure of another known or identified private person or entity shall, to the extent consistent with requirements of national security or law enforcement, notify and convey such information to such other private person or entity as soon as reasonable after

receipt of such information by the agency or authority.

(2) SCOPE OF NOTIFICATION.—Paragraph (1) may not be construed to require an agency or authority to independently investigate or determine whom to warn if information otherwise referred to in that paragraph does not identify or make known the person or entity to which the information relates.

(b) ANALYSIS OF INFORMATION.—Upon receipt of critical infrastructure information that is voluntarily submitted to the Federal Government, the Federal agency receiving such information shall—

(1) share with all covered Federal agencies (as specified in section 5(a)(2)) all such information that concerns actual attacks, and threats and warnings of attacks, on critical infrastructure and protected systems;

(2) identify interdependencies; and

(3) determine whether further analysis in concert with other Federal agencies, or warnings under subsection (c), are warranted.

(c) ACTION FOLLOWING ANALYSIS.—

(1) AUTHORITY TO ISSUE WARNINGS.—As a result of analysis of critical infrastructure information under subsection (b), a Federal agency may issue

warnings to individual companies, targeted sectors, other governmental entities, or the general public regarding potential threats to critical infrastructure.

(2) FORM OF WARNINGS.—In issuing a warning under paragraph (1), the Federal agency concerned shall take appropriate actions to prevent the disclosure of the source of any voluntarily submitted critical infrastructure information that forms the basis for the warning.

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

(1) IN GENERAL.—The President shall designate an element within the Executive Branch—

(A) to conduct strategic analyses of potential threats to critical infrastructure; and

(B) to submit reports on such analyses to Information Sharing and Analysis Organizations and such other entities as the President considers appropriate.

(2) STRATEGIC ANALYSES.—

(A) INFORMATION USED.—In conducting strategic analyses under paragraph (1)(A), the element designated to conduct such analyses under paragraph (1) shall utilize a range of critical infrastructure information voluntarily

submitted to the Federal Government by the private sector, as well as applicable intelligence and law enforcement information.

(B) AVAILABILITY.—The President shall take appropriate actions to ensure that, to the maximum extent practicable, all critical infrastructure information voluntarily submitted to the Federal Government by the private sector is available to the element designated under paragraph (1) to conduct strategic analyses under paragraph (1)(A).

(C) FREQUENCY.—Strategic analyses shall be conducted under this paragraph with such frequency as the President considers appropriate, and otherwise specifically at the direction of the President.

(3) REPORTS.—

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

(i) A description of currently recognized methods of attacks on critical infrastructure.

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

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

(iv) Such other information on the protection of critical infrastructure as the element conducting analyses under paragraph (1) considers appropriate.

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

(4) CONSTRUCTION.—Nothing in this subsection shall be construed to modify or alter any responsibility of a Federal agency under subsections (a) through (c).

SEC. 7. ANTITRUST EXEMPTION FOR ACTIVITY INVOLVING AGREEMENTS ON CRITICAL INFRASTRUCTURE MATTERS.

(a) ANTITRUST EXEMPTION.—The antitrust laws shall not apply to conduct engaged in by an Information Sharing and Analysis Organization or its members, including making and implementing an agreement, solely for purposes of—

(1) gathering and analyzing critical infrastructure information in order to better understand security problems related to critical infrastructure and

protected systems, and interdependencies of critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability of critical infrastructure and protected systems;

(2) communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a problem related to critical infrastructure or protected systems; or

(3) voluntarily disseminating critical infrastructure information to entity members, other Information Sharing and Analysis Organizations, the Federal Government, or any entities which may be of assistance in carrying out the purposes specified in paragraphs (1) and (2).

(b) EXCEPTION.—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.

(c) ANTITRUST LAWS DEFINED.—In this section, the term ''antitrust laws''—

(1) has the meaning given such term 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

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

SEC. 8. NO PRIVATE RIGHT OF ACTION.

Nothing in this Act may be construed to create a private right of action for enforcement of any provision of this Act.