Homeland Security Act
H.R. 5005
November, 2002

One Hundred Seventh Congress of the United States of America AT THE SECOND SESSION

Begun and held at the City of Washington on Wednesday, the twenty-third day of January, two thousand and two

An Act To establish the Department of Homeland Security, and for other purposes.

***

TITLE II--INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

***

SEC. 202. ACCESS TO INFORMATION.

(a) IN GENERAL-

(1) THREAT AND VULNERABILITY INFORMATION- Except as otherwise directed by the President, the Secretary shall have such access as the Secretary considers necessary to all information, including reports, assessments, analyses, and unevaluated intelligence relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary, and to all information concerning infrastructure or other vulnerabilities of the United States to terrorism, whether or not such information has been analyzed, that may be collected, possessed, or prepared by any agency of the Federal Government.

(2) OTHER INFORMATION- The Secretary shall also have access to other information relating to matters under the responsibility of the Secretary that may be collected, possessed, or prepared by an agency of the Federal Government as the President may further provide.

(b) MANNER OF ACCESS- Except as otherwise directed by the President, with respect to information to which the Secretary has access pursuant to this section--

(1) the Secretary may obtain such material upon request, and may enter into cooperative arrangements with other executive agencies to provide such material or provide Department officials with access to it on a regular or routine basis, including requests or arrangements involving broad categories of material, access to electronic databases, or both; and

(2) regardless of whether the Secretary has made any request or entered into any cooperative arrangement pursuant to paragraph (1), all agencies of the Federal Government shall promptly provide to the Secretary--

(A) all reports (including information reports containing intelligence which has not been fully evaluated), assessments, and analytical information relating to threats of terrorism against the United States and to other areas of responsibility assigned by the Secretary;

(B) all information concerning the vulnerability of the infrastructure of the United States, or other vulnerabilities of the United States, to terrorism, whether or not such information has been analyzed;

(C) all other information relating to significant and credible threats of terrorism against the United States, whether or not such information has been analyzed; and

(D) such other information or material as the President may direct.

(c) TREATMENT UNDER CERTAIN LAWS- The Secretary shall be deemed to be a Federal law enforcement, intelligence, protective, national defense, immigration, or national security official, and shall be provided with all information from law enforcement agencies that is required to be given to the Director of Central Intelligence, under any provision of the following:

(1) The USA PATRIOT Act of 2001 (Public Law 107-56).

(2) Section 2517(6) of title 18, United States Code.

(3) Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure.

(d) ACCESS TO INTELLIGENCE AND OTHER INFORMATION-

(1) ACCESS BY ELEMENTS OF FEDERAL GOVERNMENT- Nothing in this title shall preclude any element of the intelligence community (as that term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)), or any other element of the Federal Government with responsibility for analyzing terrorist threat information, from receiving any intelligence or other information relating to terrorism.

(2) SHARING OF INFORMATION- The Secretary, in consultation with the Director of Central Intelligence, shall work to ensure that intelligence or other information relating to terrorism to which the Department has access is appropriately shared with the elements of the Federal Government referred to in paragraph (1), as well as with State and local governments, as appropriate.

Subtitle B--Critical Infrastructure Information

***

SEC. 214. PROTECTION OF VOLUNTARILY SHARED CRITICAL INFRASTRUCTURE INFORMATION.

(a) PROTECTION-

(1) IN GENERAL- Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (2)--

(A) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act);

(B) shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official;

(C) shall not, without the written consent of the person or entity submitting such information, be used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith;

(D) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this subtitle, except--

(i) in furtherance of an investigation or the prosecution of a criminal act; or

(ii) when disclosure of the information would be--

(I) to either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(II) to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the General Accounting Office.

(E) shall not, if provided to a State or local government or government agency--

(i) be made available pursuant to any State or local law requiring disclosure of information or records;

(ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the written consent of the person or entity submitting such information; or

(iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act; and

(F) does not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection.

(2) 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 substantially similar to the following: `This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002.'; or

(B) in the case of oral information, a similar written statement submitted within a reasonable period following the oral communication.

(b) LIMITATION- No communication of critical infrastructure information to a covered Federal agency made pursuant to this subtitle shall be considered to be an action subject to the requirements of the Federal Advisory Committee Act (5 U.S.C. App. 2).

(c) INDEPENDENTLY OBTAINED INFORMATION- Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or authority, or any third party, under applicable law, to obtain critical infrastructure information in a manner not covered by subsection (a), including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law.

(d) TREATMENT OF VOLUNTARY SUBMITTAL OF INFORMATION- The voluntary submittal to the Government of information or records that are protected from disclosure by this subtitle 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 Secretary of the Department of Homeland Security shall, in consultation with appropriate representatives of the National Security Council and the Office of Science and Technology Policy, establish uniform procedures for the receipt, care, and storage by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government. The procedures shall be established not later than 90 days after the date of the enactment of this subtitle.

(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 Government;

(B) the maintenance of the identification of such information as voluntarily submitted to the Government for purposes of and subject to the provisions of this subtitle;

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

(D) the protection and maintenance of the confidentiality of such information so as to permit the sharing of such information within the Federal Government and with State and local governments, and the issuance of notices and warnings related to the protection of critical infrastructure and protected systems, in such manner as to protect from public disclosure the identity of the submitting person or entity, or information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is otherwise not appropriately in the public domain.

(f) PENALTIES- Whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any critical infrastructure information protected from disclosure by this subtitle coming to him in the course of this employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18 of the United States Code, imprisoned not more than 1 year, or both, and shall be removed from office or employment.

(g) AUTHORITY TO ISSUE WARNINGS- The Federal Government may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, or the general public regarding potential threats to critical infrastructure as appropriate. In issuing a warning, the Federal Government shall take appropriate actions to protect from disclosure--

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

(2) information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

(h) AUTHORITY TO DELEGATE- The President may delegate authority to a critical infrastructure protection program, designated under section 213, to enter into a voluntary agreement to promote critical infrastructure security, including with any Information Sharing and Analysis Organization, or a plan of action as otherwise defined in section 708 of the Defense Production Act of 1950 (50 U.S.C. App. 2158).
***
Subtitle C--Information Security

SEC. 221. PROCEDURES FOR SHARING INFORMATION.

The Secretary shall establish procedures on the use of information shared under this title that--

(1) limit the redissemination of such information to ensure that it is not used for an unauthorized purpose;

(2) ensure the security and confidentiality of such information;

(3) protect the constitutional and statutory rights of any individuals who are subjects of such information; and

(4) provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

SEC. 222. PRIVACY OFFICER.

The Secretary shall appoint a senior official in the Department to assume primary responsibility for privacy policy, including--

(1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;

(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;

(4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected; and

(5) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters.

***

SEC. 225. CYBER SECURITY ENHANCEMENT ACT OF 2002.

(a) SHORT TITLE- This section may be cited as the `Cyber Security Enhancement Act of 2002'.

(b) AMENDMENT OF SENTENCING GUIDELINES RELATING TO CERTAIN COMPUTER CRIMES-

(1) DIRECTIVE TO THE UNITED STATES SENTENCING COMMISSION- Pursuant to its authority under section 994(p) of title 28, United States Code, and in accordance with this subsection, the United States Sentencing Commission shall review and, if appropriate, amend its guidelines and its policy statements applicable to persons convicted of an offense under section 1030 of title 18, United States Code.

(2) REQUIREMENTS- In carrying out this subsection, the Sentencing Commission shall--

(A) ensure that the sentencing guidelines and policy statements reflect the serious nature of the offenses described in paragraph (1), the growing incidence of such offenses, and the need for an effective deterrent and appropriate punishment to prevent such offenses;

(B) consider the following factors and the extent to which the guidelines may or may not account for them--

(i) the potential and actual loss resulting from the offense;

(ii) the level of sophistication and planning involved in the offense;

(iii) whether the offense was committed for purposes of commercial advantage or private financial benefit;

(iv) whether the defendant acted with malicious intent to cause harm in committing the offense;

(v) the extent to which the offense violated the privacy rights of individuals harmed;

(vi) whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice;

(vii) whether the violation was intended to or had the effect of significantly interfering with or disrupting a critical infrastructure; and

(viii) whether the violation was intended to or had the effect of creating a threat to public health or safety,
or injury to any person;

(C) assure reasonable consistency with other relevant directives and with other sentencing guidelines;

(D) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(E) make any necessary conforming changes to the sentencing guidelines; and

(F) assure that the guidelines adequately meet the purposes of sentencing as set forth in section 3553(a)(2) of title 18, United States Code.

(c) STUDY AND REPORT ON COMPUTER CRIMES- Not later than May 1, 2003, the United States Sentencing Commission shall submit a brief report to Congress that explains any actions taken by the Sentencing Commission in response to this section and includes any recommendations the Commission may have regarding statutory penalties for offenses under section 1030 of title 18, United States Code.

(d) EMERGENCY DISCLOSURE EXCEPTION-

(1) IN GENERAL- Section 2702(b) of title 18, United States Code, is amended--

(A) in paragraph (5), by striking `or' at the end;

(B) in paragraph (6)(A), by inserting `or' at the end;

(C) by striking paragraph (6)(C); and

(D) by adding at the end the following:

`(7) to a Federal, State, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.'.

(2) REPORTING OF DISCLOSURES- A government entity that receives a disclosure under section 2702(b) of title 18, United States Code, shall file, not later than 90 days after such disclosure, a report to the Attorney General stating the paragraph of that section under which the disclosure was made, the date of the disclosure, the entity to which the disclosure was made, the number of customers or subscribers to whom the information disclosed pertained, and the number of communications, if any, that were disclosed. The Attorney General shall publish all such reports into a single report to be submitted to Congress 1 year after the date of enactment of this Act.

(e) GOOD FAITH EXCEPTION- Section 2520(d)(3) of title 18, United States Code, is amended by inserting `or 2511(2)(i)' after `2511(3)'.

(f) INTERNET ADVERTISING OF ILLEGAL DEVICES- Section 2512(1)(c) of title 18, United States Code, is amended--

(1) by inserting `or disseminates by electronic means' after `or other publication'; and

(2) by inserting `knowing the content of the advertisement and' before `knowing or having reason to know'.

(g) STRENGTHENING PENALTIES- Section 1030(c) of title 18, United States Code, is amended--

(1) by striking `and' at the end of paragraph (3);

(2) in each of subparagraphs (A) and (C) of paragraph (4), by inserting `except as provided in paragraph (5),' before `a fine under this title';

(3) in paragraph (4)(C), by striking the period at the end and inserting `; and'; and

(4) by adding at the end the following:

`(5)(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and

`(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.'.

(h) PROVIDER ASSISTANCE-

(1) SECTION 2703- Section 2703(e) of title 18, United States Code, is amended by inserting `, statutory authorization' after `subpoena'.

(2) SECTION 2511- Section 2511(2)(a)(ii) of title 18, United States Code, is amended by inserting `, statutory authorization,' after `court order' the last place it appears.

(i) EMERGENCIES- Section 3125(a)(1) of title 18, United States Code, is amended--

(1) in subparagraph (A), by striking `or' at the end;

(2) in subparagraph (B), by striking the comma at the end and inserting a semicolon; and

(3) by adding at the end the following:

`(C) an immediate threat to a national security interest; or

`(D) an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year;'.

(j) PROTECTING PRIVACY-

(1) SECTION 2511- Section 2511(4) of title 18, United States Code, is amended--

(A) by striking paragraph (b); and

(B) by redesignating paragraph (c) as paragraph (b).

(2) SECTION 2701- Section 2701(b) of title 18, United States Code, is amended--

(A) in paragraph (1), by inserting `, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State' after `commercial gain';

(B) in paragraph (1)(A), by striking `one year' and inserting `5 years';

(C) in paragraph (1)(B), by striking `two years' and inserting `10 years'; and

(D) by striking paragraph (2) and inserting the following:

`(2) in any other case--

`(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

`(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.'.

***

SEC. 1514. NATIONAL IDENTIFICATION SYSTEM NOT AUTHORIZED.

Nothing in this Act shall be construed to authorize the development of a national identification system or card.