TITLE II--INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

Subtitle A--Directorate for Information Analysis and Infrastructure Protection; Access to Information

SEC. 201. DIRECTORATE FOR INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION.

(a) UNDER SECRETARY OF HOMELAND SECURITY FOR INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION-

(1) IN GENERAL- There shall be in the Department a Directorate for Information Analysis and Infrastructure Protection headed by an Under Secretary for Information Analysis and Infrastructure Protection, who shall be appointed by the President, by and with the advice and consent of the Senate.

(2) RESPONSIBILITIES- The Under Secretary shall assist the Secretary in discharging the responsibilities assigned by the Secretary.

(b) ASSISTANT SECRETARY FOR INFORMATION ANALYSIS; ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION-

(1) ASSISTANT SECRETARY FOR INFORMATION ANALYSIS- There shall be in the Department an Assistant Secretary for Information Analysis, who shall be appointed by the President.

(2) ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION- There shall be in the Department an Assistant Secretary for Infrastructure Protection, who shall be appointed by the President.

(3) RESPONSIBILITIES- The Assistant Secretary for Information Analysis and the Assistant Secretary for Infrastructure Protection shall assist the Under Secretary for Information Analysis and Infrastructure Protection in discharging the responsibilities of the Under Secretary under this section.

(c) DISCHARGE OF INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION-

The Secretary shall ensure that the responsibilities of the Department regarding information analysis and infrastructure protection are carried out through the Under Secretary for Information Analysis and Infrastructure Protection.

(d) RESPONSIBILITIES OF UNDER SECRETARY- Subject to the direction and control of the Secretary, the responsibilities of the Under Secretary

for Information Analysis and Infrastructure Protection shall be as follows:

(1) To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information in order to--

(A) identify and assess the nature and scope of terrorist threats to the homeland;

(B) detect and identify threats of terrorism against the United States; and

(C) understand such threats in light of actual and potential vulnerabilities of the homeland.

(2) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks).

(3) To integrate relevant information, analyses, and vulnerability assessments (whether such information, analyses, or assessments are provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities.

(4) To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this section, including obtaining such information from other agencies of the Federal Government.

(5) To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency preparedness communications systems, and the physical and technological assets that support such systems.

(6) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination

with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.

(7) To administer the Homeland Security Advisory System, including--

(A) exercising primary responsibility for public advisories related to threats to homeland security; and

(B) in coordination with other agencies of the Federal Government, providing specific warning information, and advice about appropriate protective measures and countermeasures, to State and local government agencies and authorities, the private sector, other entities, and the public.

(8) To review, analyze, and make recommendations for improvements in the policies and procedures governing the sharing of law enforcement information, intelligence information, intelligence-related information, and other information relating to homeland security within the Federal Government and between the Federal Government and State and local government agencies and authorities.

(9) To disseminate, as appropriate, information analyzed by the Department within the Department, to other agencies of the Federal Government with responsibilities relating to homeland security, and to agencies of State and local governments and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.

(10) To consult with the Director of Central Intelligence and other appropriate intelligence, law enforcement, or other elements of the Federal Government to establish collection priorities and strategies for information, including law enforcement-related information, relating to threats of terrorism against the United States through such means as the representation of the Department in discussions regarding requirements and priorities in the collection of such information.

(11) To consult with State and local governments and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

(12) To ensure that--

(A) any material received pursuant to this Act is protected

from unauthorized disclosure and handled and used only for the performance of official duties; and

(B) any intelligence information under this Act is shared, retained, and disseminated consistent with the authority of the Director of Central Intelligence to protect intelligence sources and methods under the National Security Act of 1947 (50 U.S.C. 401 et seq.) and related procedures and, as appropriate, similar authorities of the Attorney General concerning sensitive law enforcement information.

(13) To request additional information from other agencies of the Federal Government, State and local government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

(14) To establish and utilize, in conjunction with the chief information officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

(15) To ensure, in conjunction with the chief information officer of the Department, that any information databases and analytical tools developed or utilized by the Department--

(A) are compatible with one another and with relevant information databases of other agencies of the Federal Government; and

(B) treat information in such databases in a manner that complies with applicable Federal law on privacy.

(16) To coordinate training and other support to the elements and personnel of the Department, other agencies of the Federal Government, and State and local governments that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

(17) To coordinate with elements of the intelligence community and with Federal, State, and local law enforcement agencies, and the private sector, as appropriate.

(18) To provide intelligence and information analysis and support to other elements of the Department.

(19) To perform such other duties relating to such responsibilities as the Secretary may provide.

(e) STAFF-

(1) IN GENERAL- The Secretary shall provide the Directorate with a staff of analysts having appropriate expertise and experience to assist the Directorate in discharging responsibilities under this section.

(2) PRIVATE SECTOR ANALYSTS- Analysts under this subsection may include analysts from the private sector.

(3) SECURITY CLEARANCES- Analysts under this subsection shall possess security clearances appropriate for their work under this section.

(f) DETAIL OF PERSONNEL-

(1) IN GENERAL- In order to assist the Directorate in discharging responsibilities under this section, personnel of the agencies referred to in paragraph (2) may be detailed to the Department for the performance of analytic functions and related duties.

(2) COVERED AGENCIES- The agencies referred to in this paragraph are as follows:

(A) The Department of State.

(B) The Central Intelligence Agency.

(C) The Federal Bureau of Investigation.

(D) The National Security Agency.

(E) The National Imagery and Mapping Agency.

(F) The Defense Intelligence Agency.

(G) Any other agency of the Federal Government that the President considers appropriate.

(3) COOPERATIVE AGREEMENTS- The Secretary and the head of the agency concerned may enter into cooperative agreements for the purpose of detailing personnel under this subsection.

(4) BASIS- The detail of personnel under this subsection may be on a reimbursable or non-reimbursable basis.

(g) FUNCTIONS TRANSFERRED- In accordance with title XV, there shall be transferred to the Secretary, for assignment to the Under Secretary for Information Analysis and Infrastructure Protection under this section, the functions, personnel, assets, and liabilities of the following:

(1) The National Infrastructure Protection Center of the Federal Bureau of Investigation (other than the Computer Investigations and Operations Section), including the functions of the Attorney General relating thereto.

(2) The National Communications System of the Department of Defense, including the functions of the Secretary of Defense relating thereto.

(3) The Critical Infrastructure Assurance Office of the Department of Commerce, including the functions of the Secretary of Commerce relating thereto.

(4) The National Infrastructure Simulation and Analysis Center of the Department of Energy and the energy security and assurance program and activities of the Department, including the functions of the Secretary of Energy relating thereto.

(5) The Federal Computer Incident Response Center of the General Services Administration, including the functions of the Administrator of General Services relating thereto.

(h) INCLUSION OF CERTAIN ELEMENTS OF THE DEPARTMENT AS ELEMENTS OF THE
INTELLIGENCE COMMUNITY- Section 3(4) of the National Security Act of 1947 (50 U.S.C. 401(a)) is amended--

(1) by striking `and' at the end of subparagraph (I);

(2) by redesignating subparagraph (J) as subparagraph (K); and

(3) by inserting after subparagraph (I) the following new subparagraph:

`(J) the elements of the Department of Homeland Security concerned with the analyses of foreign intelligence information; and'.

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 other any 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. 211. SHORT TITLE.

This subtitle may be cited as the `Critical Infrastructure Information Act of 2002'.

SEC. 212. DEFINITIONS.

In this subtitle:

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

(2) COVERED FEDERAL AGENCY- The term `covered Federal agency' means the Department of Homeland Security.

(3) CRITICAL INFRASTRUCTURE INFORMATION- The term `critical infrastructure information' means information not customarily in the public domain and related to the security of critical infrastructure or protected systems--

(A) actual, potential, or threatened interference with,

attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

(4) CRITICAL INFRASTRUCTURE PROTECTION PROGRAM- The term `critical infrastructure protection program' means any component or bureau of a covered Federal agency that has been designated by the President or any agency head to receive critical infrastructure information.

(5) INFORMATION SHARING AND ANALYSIS ORGANIZATION- The term `Information Sharing and Analysis Organization' means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of--

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

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

(C) voluntarily disseminating critical infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

(6) PROTECTED SYSTEM- The term `protected system'--

(A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of 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 the medium of transmission or storage.

(7) VOLUNTARY-

(A) IN GENERAL- The term `voluntary', in the case of any submittal of critical infrastructure information to a covered Federal agency, means the submittal thereof in the absence of such agency's exercise of legal authority to compel access to or submission of such information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.

(B) EXCLUSIONS- The term `voluntary'--

(i) in the case of any action brought under the securities laws as is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47))--

(I) does not include information or statements contained in any documents or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 781(I)); and

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

(ii) does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.

SEC. 213. DESIGNATION OF CRITICAL INFRASTRUCTURE PROTECTION PROGRAM.

A critical infrastructure protection program may be designated as such by one of the following:

(1) The President.

(2) The Secretary of Homeland Security.

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).

SEC. 215. NO PRIVATE RIGHT OF ACTION.

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

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. 223. ENHANCEMENT OF NON-FEDERAL CYBERSECURITY.

In carrying out the responsibilities under section 201, the Under Secretary for Information Analysis and Infrastructure Protection shall--

(1) as appropriate, provide to State and local government entities, and upon request to private entities that own or operate critical information systems--

(A) analysis and warnings related to threats to, and vulnerabilities of, critical information systems; and

(B) in coordination with the Under Secretary for Emergency Preparedness and Response, crisis management support in response to threats to, or attacks on, critical information systems; and

(2) as appropriate, provide technical assistance, upon request, to the private sector and other government entities, in coordination with the Under Secretary for Emergency Preparedness and Response, with respect to emergency recovery plans to respond to major failures of critical information systems.

SEC. 224. NET GUARD.

The Under Secretary for Information Analysis and Infrastructure Protection may establish a national technology guard, to be known as `NET Guard', comprised of local teams of volunteers with expertise in relevant areas of science and technology, to assist local communities to respond and recover from attacks on information systems and communications networks.

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.'.

Subtitle D--Office of Science and Technology

SEC. 231. ESTABLISHMENT OF OFFICE; DIRECTOR.

(a) ESTABLISHMENT-

(1) IN GENERAL- There is hereby established within the Department of Justice an Office of Science and Technology (hereinafter in this title referred to as the `Office').

(2) AUTHORITY- The Office shall be under the general authority of the Assistant Attorney General, Office of Justice Programs, and shall be established within the National Institute of Justice.

(b) DIRECTOR- The Office shall be headed by a Director, who shall be an individual appointed based on approval by the Office of Personnel Management of the executive qualifications of the individual.

SEC. 232. MISSION OF OFFICE; DUTIES.

(a) MISSION- The mission of the Office shall be--

(1) to serve as the national focal point for work on law enforcement technology; and

(2) to carry out programs that, through the provision of equipment, training, and technical assistance, improve the safety and effectiveness of law enforcement technology and improve access to such technology by Federal, State, and local law enforcement agencies.

(b) DUTIES- In carrying out its mission, the Office shall have the following duties:

(1) To provide recommendations and advice to the Attorney General.

(2) To establish and maintain advisory groups (which shall be exempt from the provisions of the Federal Advisory Committee Act (5 U.S.C. App.)) to assess the law enforcement technology needs of Federal, State, and local law enforcement agencies.

(3) To establish and maintain performance standards in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113) for, and test and evaluate law enforcement technologies that may be used by, Federal, State, and local law enforcement agencies.

(4) To establish and maintain a program to certify, validate, and mark or otherwise recognize law enforcement technology products that conform to standards established and maintained by the Office in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113). The program may, at the discretion of the Office, allow for supplier's declaration of conformity with such standards.

(5) To work with other entities within the Department of Justice, other Federal agencies, and the executive office of the President to establish a coordinated Federal approach on issues related to law enforcement technology.

(6) To carry out research, development, testing, evaluation, and cost-benefit analyses in fields that would improve the safety, effectiveness, and efficiency of law enforcement technologies used by Federal, State, and local law enforcement agencies, including, but not limited to--

(A) weapons capable of preventing use by unauthorized persons, including personalized guns;

(B) protective apparel;

(C) bullet-resistant and explosion-resistant glass;

(D) monitoring systems and alarm systems capable of providing precise location information;

(E) wire and wireless interoperable communication technologies;

(F) tools and techniques that facilitate investigative and forensic work, including computer forensics;

(G) equipment for particular use in counterterrorism, including devices and technologies to disable terrorist devices;

(H) guides to assist State and local law enforcement agencies;

(I) DNA identification technologies; and

(J) tools and techniques that facilitate investigations of computer crime.

(7) To administer a program of research, development, testing, and demonstration to improve the interoperability of voice and data public safety communications.

(8) To serve on the Technical Support Working Group of the Department of Defense, and on other relevant interagency panels, as requested.

(9) To develop, and disseminate to State and local law enforcement agencies, technical assistance and training materials for law enforcement personnel, including prosecutors.

(10) To operate the regional National Law Enforcement and Corrections Technology Centers and, to the extent necessary, establish additional centers through a competitive process.

(11) To administer a program of acquisition, research, development, and dissemination of advanced investigative analysis and forensic tools to assist State and local law enforcement agencies in combating cybercrime.

(12) To support research fellowships in support of its mission.

(13) To serve as a clearinghouse for information on law enforcement technologies.

(14) To represent the United States and State and local law enforcement agencies, as requested, in international activities concerning law enforcement technology.

(15) To enter into contracts and cooperative agreements and provide grants, which may require in-kind or cash matches from the recipient, as necessary to carry out its mission.

(16) To carry out other duties assigned by the Attorney General to accomplish the mission of the Office.

(c) COMPETITION REQUIRED- Except as otherwise expressly provided by law, all research and development carried out by or through the Office shall be carried out on a competitive basis.

(d) INFORMATION FROM FEDERAL AGENCIES- Federal agencies shall, upon request from the Office and in accordance with Federal law, provide the Office with any data, reports, or other information requested, unless compliance with such request is otherwise prohibited by law.

(e) PUBLICATIONS- Decisions concerning publications issued by the Office shall rest solely with the Director of the Office.

(f) TRANSFER OF FUNDS- The Office may transfer funds to other Federal agencies or provide funding to non-Federal entities through grants, cooperative agreements, or contracts to carry out its duties under this section.

(g) ANNUAL REPORT- The Director of the Office shall include with the budget justification materials submitted to Congress in support of the Department of Justice budget for each fiscal year (as submitted with the budget of the President under section 1105(a) of title 31, United States Code) a report on the activities of the Office. Each such report shall include the following:

(1) For the period of 5 fiscal years beginning with the fiscal year for which the budget is submitted--

(A) the Director's assessment of the needs of Federal, State, and local law enforcement agencies for assistance with respect to law enforcement technology and other matters consistent with the mission of the Office; and

(B) a strategic plan for meeting such needs of such law enforcement agencies.

(2) For the fiscal year preceding the fiscal year for which such budget is submitted, a description of the activities carried out by the Office and an evaluation of the extent to which those activities successfully meet the needs assessed under paragraph (1)(A) in previous reports.

SEC. 233. DEFINITION OF LAW ENFORCEMENT TECHNOLOGY.

For the purposes of this title, the term `law enforcement technology' includes investigative and forensic technologies, corrections technologies, and technologies that support the judicial process.

SEC. 234. ABOLISHMENT OF OFFICE OF SCIENCE AND TECHNOLOGY OF NATIONAL
INSTITUTE OF JUSTICE; TRANSFER OF FUNCTIONS.

(a) AUTHORITY TO TRANSFER FUNCTIONS- The Attorney General may transfer to the Office any other program or activity of the Department of Justice that the Attorney General, in consultation with the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives, determines to be consistent with the mission of the Office.

(b) TRANSFER OF PERSONNEL AND ASSETS- With respect to any function, power, or duty, or any program or activity, that is established in the Office, those employees and assets of the element of the Department of Justice from which the transfer is made that the Attorney General

determines are needed to perform that function, power, or duty, or for that program or activity, as the case may be, shall be transferred to the Office.

(c) REPORT ON IMPLEMENTATION- Not later than 1 year after the date of the enactment of this Act, the Attorney General shall submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a report on the implementation of this title. The report shall--

(1) provide an accounting of the amounts and sources of funding available to the Office to carry out its mission under existing authorizations and appropriations, and set forth the future funding needs of the Office; and

(2) include such other information and recommendations as the Attorney General considers appropriate.

SEC. 235. NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTERS.

(a) IN GENERAL- The Director of the Office shall operate and support National Law Enforcement and Corrections Technology Centers (hereinafter in this section referred to as `Centers') and, to the extent necessary, establish new centers through a merit-based, competitive process.

(b) PURPOSE OF CENTERS- The purpose of the Centers shall be to--

(1) support research and development of law enforcement technology;

(2) support the transfer and implementation of technology;

(3) assist in the development and dissemination of guidelines and technological standards; and

(4) provide technology assistance, information, and support for law enforcement, corrections, and criminal justice purposes.

(c) ANNUAL MEETING- Each year, the Director shall convene a meeting of the Centers in order to foster collaboration and communication between Center participants.

(d) REPORT- Not later than 12 months after the date of the enactment of this Act, the Director shall transmit to the Congress a report assessing the effectiveness of the existing system of Centers and identify the number of Centers necessary to meet the technology needs of Federal, State, and local law enforcement in the United States.

SEC. 236. COORDINATION WITH OTHER ENTITIES WITHIN DEPARTMENT OF JUSTICE.

Section 102 of the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. 3712) is amended in subsection (a)(5) by inserting `coordinate and' before `provide'.

SEC. 237. AMENDMENTS RELATING TO NATIONAL INSTITUTE OF JUSTICE.

Section 202(c) of the Omnibus Crime Control and Safety Streets Act of 1968 (42 U.S.C. 3722(c)) is amended--

(1) in paragraph (3) by inserting `, including cost effectiveness where practical,' before `of projects'; and

(2) by striking `and' after the semicolon at the end of paragraph (8), striking the period at the end of paragraph (9) and inserting `; and', and by adding at the end the following:

`(10) research and development of tools and technologies relating to prevention, detection, investigation, and prosecution of crime; and

`(11) support research, development, testing, training, and evaluation of tools and technology for Federal, State, and local law enforcement agencies.'.