Computer Crime and Intellectual Property Section (CCIPS)

Email this Document!

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I - CRIMES
CHAPTER 47 - FRAUD AND FALSE STATEMENTS

---

§ 1030. Fraud and related activity in connection with computers

(a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not

exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)(A)***(i)*** knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

~~(B)~~ ***(ii)*** intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

~~(C)~~ ***(iii)*** intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person, ~~firm, association, educational institution, financial institution, government entity, or other legal entity,~~ any money or other thing of value, transmits

in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is--

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)(A) ***except as provided in subparagraph (B)***, a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), ~~(a)(5)(C)~~ ***(a)(5)(A)(iii)***, or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), ***or an attempt to commit an offense punishable under this subparagraph,*** if–

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000;

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; ~~and~~

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection ~~(a)(4), (a)(5)(A), (a)(5)(B),~~ or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), ~~(a)(5)(A), (a)(5)(B), (a)(5)(C)~~ ***(a)(5)(A)(iii),*** or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(4)(A) a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

(C) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section.

~~(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.~~

(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section--

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer--
(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication, ***including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;***

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means--

(A) an institution with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act.

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5; and

~~(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information, that--~~

~~(A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals;~~

~~(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;~~

~~(C) causes physical injury to any person; or~~

~~(D) threatens public health or safety; and~~

(8) the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country.;

(10) the term 'conviction' shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term 'loss' includes any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term 'person' means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. ~~Damages for violations involving damage as defined in subsection (e)(8)(A) are limited to economic damages.~~ **A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages.** No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the

date of the discovery of the damage. **No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.**

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

Section 814(e) Amendment of sentencing guidelines relating to certain computer fraud and abuse.--

Pursuant to its authority under section 994(p) of title 28, United States Code, the United States Sentencing Commission shall amend the Federal sentencing guidelines to ensure that any individual convicted of a violation of section 1030 of title 18, United States Code, can be subjected to appropriate penalties, without regard to any mandatory minimum term of imprisonment.

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I--CRIMES
CHAPTER 96--RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS

§ 1961. Definitions

As used in this chapter--

(1) "racketeering activity" means (A) any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in obscene matter, or dealing in a controlled substance or listed chemical (as defined in section 102 of the Controlled Substances Act), which is chargeable under State law and punishable by imprisonment for more than one year; (B) any act which is indictable under any of the following provisions of title 18, United States Code: Section 201 (relating to bribery), section 224 (relating to sports bribery), sections 471, 472, and 473 (relating to counterfeiting), section 659 (relating to theft from interstate shipment) if the act indictable under section 659 is felonious, section 664 (relating to embezzlement from pension and welfare funds), sections 891-894 (relating to extortionate credit transactions), section 1028 (relating to fraud and related activity in connection with identification documents), section 1029 (relating to fraud and related activity in connection with access devices), section 1084 (relating to the transmission of gambling information), section 1341 (relating to mail fraud), section 1343 (relating to wire fraud), section 1344 (relating to financial institution fraud), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of

naturalization or citizenship papers), sections 1461-1465 (relating to obscene matter), section 1503 (relating to obstruction of justice), section 1510 (relating to obstruction of criminal investigations), section 1511 (relating to the obstruction of State or local law enforcement), section 1512 (relating to tampering with a witness, victim, or an informant), section 1513 (relating to retaliating against a witness, victim, or an informant), section 1542 (relating to false statement in application and use of passport), section 1543 (relating to forgery or false use of passport), section 1544 (relating to misuse of passport), section 1546 (relating to fraud and misuse of visas, permits, and other documents), sections 1581-1588 (relating to peonage and slavery), section 1951 (relating to interference with commerce, robbery, or extortion), section 1952 (relating to racketeering), section 1953 (relating to interstate transportation of wagering paraphernalia), section 1954 (relating to unlawful welfare fund payments), section 1955 (relating to the prohibition of illegal gambling businesses), section 1956 (relating to the laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 1958 (relating to use of interstate commerce facilities in the commission of murder-for-hire), sections 2251, 2251A, 2252, and 2260 (relating to sexual exploitation of children), sections 2312 and 2313 (relating to interstate transportation of stolen motor vehicles), sections 2314 and 2315 (relating to interstate transportation of stolen property), section 2318 (relating to trafficking in counterfeit labels for phonorecords, computer programs or computer program documentation or packaging and copies of motion pictures or other audiovisual works), section 2319 (relating to criminal infringement of a copyright), section 2319A (relating to unauthorized fixation of and trafficking in sound recordings and music videos of live musical performances), section 2320 (relating to trafficking in goods or services bearing counterfeit marks), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), sections 2341-2346 (relating to trafficking in contraband cigarettes), sections 2421-24 (relating to white slave traffic), (C) any act which is indictable under title 29, United States Code, section 186 (dealing with restrictions on payments and loans to labor organizations) or section 501(c) (relating to embezzlement from union funds), (D) any offense involving fraud connected with a case under title 11 (except a case under section 157 of this title), fraud in the sale of securities, or the felonious manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in a controlled substance or listed chemical (as defined in section 102 of the Controlled Substances Act), punishable under any law of the United States, (E) any act which is indictable under the Currency and Foreign Transactions Reporting Act, ~~or (F)~~ ***(F)*** any act which is indictable under the Immigration and Nationality Act, section 274 (relating to bringing in and harboring certain aliens), section 277 (relating to aiding or assisting certain aliens to enter the United States), or section 278 (relating to importation of alien for immoral purpose) if the act indictable under such section of such Act was committed for the purpose of financial gain, ***or (G) any act that is indictable under any provision listed in section 2332b(g)(5)(B);***

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I--CRIMES
CHAPTER 113B--TERRORISM

§ 2331. Definitions

As used in this chapter--

(1) the term "international terrorism" means activities that--

(A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;

(B) appear to be intended--

(i) to intimidate or coerce a civilian population;

(ii) to influence the policy of a government by intimidation or coercion; or

(iii) to affect the conduct of a government ~~by assassination or kidnapping~~ ***by mass destruction, assassination, or kidnapping;*** and

(C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum;

(2) the term "national of the United States" has the meaning given such term in section 101(a)(22) of the Immigration and Nationality Act;

(3) the term "person" means any individual or entity capable of holding a legal or beneficial interest in property; ~~and~~

(4) the term "act of war" means any act occurring in the course of--

(A) declared war;

(B) armed conflict, whether or not war has been declared, between two or more nations; or

(C) armed conflict between military forces of any origin.***; and***

~~(5) the term "domestic terrorism" means activities that~~

(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;

(B) appear to be intended–

(i) to intimidate or coerce a civilian population;

(ii) to influence the policy of a government by intimidation or coercion; or

(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and

(C) occur primarily within the territorial jurisdiction of the United States.

§ 2332b. Acts of terrorism transcending national boundaries

(a) Prohibited acts.--

(1) Offenses.--Whoever, involving conduct transcending national boundaries and in a circumstance described in subsection (b)--

(A) kills, kidnaps, maims, commits an assault resulting in serious bodily injury, or assaults with a dangerous weapon any person within the United States; or

(B) creates a substantial risk of serious bodily injury to any other person by destroying or damaging any structure, conveyance, or other real or personal property within the United States or by attempting or conspiring to destroy or damage any structure, conveyance, or other real or personal property within the United States;

in violation of the laws of any State, or the United States, shall be punished as prescribed in subsection (c).

(2) Treatment of threats, attempts and conspiracies.--Whoever threatens to commit an offense under paragraph (1), or attempts or conspires to do so, shall be punished under subsection (c).

(b) Jurisdictional bases.--

(1) Circumstances.--The circumstances referred to in subsection (a) are--

(A) the mail or any facility of interstate or foreign commerce is used in furtherance of the offense;

(B) the offense obstructs, delays, or affects interstate or foreign commerce, or would have so obstructed, delayed, or affected interstate or foreign commerce if the offense had been consummated;

(C) the victim, or intended victim, is the United States Government, a member of the uniformed services, or any official, officer, employee, or agent of the legislative, executive, or judicial branches, or of any department or agency, of the United States;

(D) the structure, conveyance, or other real or personal property is, in whole or in part, owned, possessed, or leased to the United States, or any department or agency of the United States;

(E) the offense is committed in the territorial sea (including the airspace above and the seabed and subsoil below, and artificial islands and fixed structures erected thereon) of the United States; or

(F) the offense is committed within the special maritime and territorial jurisdiction of the United States.

(2) Co-conspirators and accessories after the fact.--Jurisdiction shall exist over all principals and co-conspirators of an offense under this section, and accessories after the fact to any offense under this section, if at least one of the circumstances described in subparagraphs (A) through (F) of paragraph (1) is applicable to at least one offender.

(c) Penalties.--

(1) Penalties.--Whoever violates this section shall be punished--

(A) for a killing, or if death results to any person from any other conduct prohibited by this section, by death, or by imprisonment for any term of years or for life;

(B) for kidnapping, by imprisonment for any term of years or for life;

(C) for maiming, by imprisonment for not more than 35 years;

(D) for assault with a dangerous weapon or assault resulting in serious bodily injury, by imprisonment for not more than 30 years;

(E) for destroying or damaging any structure, conveyance, or other real or personal property, by imprisonment for not more than 25 years;
(F) for attempting or conspiring to commit an offense, for any term of years up to the maximum punishment that would have applied had the offense been completed; and

(G) for threatening to commit an offense under this section, by imprisonment for not more than 10 years.

(2) Consecutive sentence.--Notwithstanding any other provision of law, the court shall not place on probation any person convicted of a violation of this section; nor shall the term of imprisonment imposed under this section run concurrently with any other term of imprisonment.

(d) Proof requirements.--The following shall apply to prosecutions under this section:

(1) Knowledge.--The prosecution is not required to prove knowledge by any defendant of a jurisdictional base alleged in the indictment.

(2) State law.--In a prosecution under this section that is based upon the adoption of State law, only the elements of the offense under State law, and not any provisions pertaining to criminal procedure or evidence, are adopted.

(e) Extraterritorial jurisdiction.--There is extraterritorial Federal jurisdiction--

(1) over any offense under subsection (a), including any threat, attempt, or conspiracy to commit such offense; and

(2) over conduct which, under section 3, renders any person an accessory after the fact to an offense under subsection (a).

(f) Investigative authority.--In addition to any other investigative authority with respect to violations of this title, the Attorney General shall have primary investigative responsibility for all Federal crimes of terrorism, ***and any violation of section 351(e), 844(e), 844(f)(1), 956(b), 1361, 1366(b), 1366(c), 1751(e), 2152, or 2156 of this title,*** and the Secretary of the Treasury shall assist the Attorney General at the request of the Attorney General. Nothing in this section shall be construed to interfere with the authority of the United States Secret Service under section 3056.

(g) Definitions.--As used in this section--

(1) the term "conduct transcending national boundaries" means conduct occurring outside of the United States in addition to the conduct occurring in the United States;

(2) the term "facility of interstate or foreign commerce" has the meaning given that term in section 1958(b)(2);

(3) the term "serious bodily injury" has the meaning given that term in section 1365(g)(3);

(4) the term "territorial sea of the United States" means all waters extending seaward to 12 nautical miles from the baselines of the United States, determined in accordance with international law; and

(5) the term "Federal crime of terrorism" means an offense that--

(A) is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct; and

(B) is a violation of--

~~(i) section 32 (relating to destruction of aircraft or aircraft facilities), 37 (relating to violence at international airports), 81 (relating to arson within special maritime and territorial jurisdiction), 175 (relating to biological weapons), 351 (relating to congressional, cabinet, and Supreme Court assassination, kidnapping, and assault), 831 (relating to nuclear materials), 842(m) or (n) (relating to plastic explosives), 844(e) (relating to certain bombings), 844(f) or (i) (relating to~~

~~arson and bombing of certain property), 930(c), 956 (relating to conspiracy to injure property of a foreign government), 1114 (relating to protection of officers and employees of the United States), 1116 (relating to murder or manslaughter of foreign officials, official guests, or internationally protected persons), 1203 (relating to hostage taking), 1361 (relating to injury of Government property or contracts), 1362 (relating to destruction of communication lines, stations, or systems), 1363 (relating to injury to buildings or property within special maritime and territorial jurisdiction of the United States), 1366 (relating to destruction of an energy facility), 1751 (relating to Presidential and Presidential staff assassination, kidnapping, and assault), 1992, 2152 (relating to injury of fortifications, harbor defenses, or defensive sea areas), 2155 (relating to destruction of national defense materials, premises, or utilities), 2156 (relating to production of defective national defense materials, premises, or utilities), 2280 (relating to violence against maritime navigation), 2281 (relating to violence against maritime fixed platforms), 2332 (relating to certain homicides and other violence against United States nationals occurring outside of the United States), 2332a (relating to use of weapons of mass destruction), 2332b (relating to acts of terrorism transcending national boundaries), 2332c, 2339A (relating to providing material support to terrorists), 2339B (relating to providing material support to terrorist organizations), or 2340A (relating to torture);~~

~~(ii) section 236 (relating to sabotage of nuclear facilities or fuel) of the Atomic Energy Act of 1954 (42 U.S.C. 2284); or~~

~~(iii) section 46502 (relating to aircraft piracy) or section 60123(b) (relating to destruction of interstate gas or hazardous liquid pipeline facility) of title 49.~~

(i) section 32 (relating to destruction of aircraft or aircraft facilities), 37 (relating to violence at international airports), 81 (relating to arson within special maritime and territorial jurisdiction), 175 or 175b (relating to biological weapons), 229 *(relating to chemical weapons), subsection* (a), (b), (c), or (d) of section 351 (relating to congressional, cabinet, and Supreme Court assassination and kidnaping), 831 (relating to nuclear materials), 842(m) or (n) (relating to plastic explosives), 844(f) (2) or (3) (relating to arson and bombing of Government property risking or causing death), 844(i) (relating to arson and bombing of property used in interstate commerce), 930(c) (relating to killing or attempted killing during an attack on a Federal facility with a dangerous weapon), 956(a)(1) (relating to conspiracy to murder, kidnap, or maim persons abroad), 1030(a)(1) (relating to protection of computers), 1030(a)(5)(A)(i) resulting in damage as defined in 1030(a)(5)(B)(ii) through (v) (relating to protection of computers), 1114 (relating to killing or attempted killing of officers and employees of the United States), 1116 (relating to murder or manslaughter of foreign officials, official guests, or internationally protected persons), 1203 (relating to hostage taking), 1362 (relating to destruction of communication lines, stations, or systems), 1363 (relating to injury to buildings or property within special maritime and territorial jurisdiction of the United States), 1366(a) (relating to destruction of an energy facility), 1751 (a), (b), (c), or (d) (relating to Presidential and Presidential staff assassination and kidnaping), 1992 (relating to wrecking trains), 1993 (relating to terrorist attacks and other acts of violence against mass transportation systems), 2155 (relating to destruction of national defense materials, premises, or utilities), 2280 (relating to violence against maritime navigation), 2281 (relating to violence against maritime fixed platforms),

2332 (relating to certain homicides and other violence against United States nationals occurring outside of the United States), 2332a (relating to use of weapons of mass destruction), 2332b (relating to acts of terrorism transcending national boundaries), 2339 (relating to harboring terrorists), 2339A (relating to providing material support to terrorists), 2339B (relating to providing material support to terrorist organizations), or 2340A (relating to torture) of this title;

(ii) section 236 (relating to sabotage of nuclear facilities or fuel) of the Atomic Energy Act of 1954 (42 U.S.C. 2284); or

‘‘(iii) section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with a dangerous weapon), section 46505(b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life by means of weapons, on aircraft), section 46506 if homicide or attempted homicide is involved (relating to application of certain criminal laws to acts on aircraft), or section 60123(b) (relating to destruction of interstate gas or hazardous liquid pipeline facility) of title 49.

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I--CRIMES
CHAPTER 119--WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

§ 2510. Definitions

As used in this chapter--

(1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce ~~and such term includes any electronic storage of such communication;~~

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device;

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than--

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;
(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means--

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) "communication common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) of title 47 of the United States Code;

(11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,

electromagnetic, photo electronic or photooptical system that affects interstate or foreign commerce, but does not include--

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(13) "user" means any person or entity who--

(A) uses an electronic communication service; and
(B) is duly authorized by the provider of such service to engage in such use;

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photo electronic facilities for the transmission of **wire or** electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not--

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) "electronic storage" means--

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; ~~and~~

(18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.**; ~~and~~**

(19) "foreign intelligence information" means–

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against–
(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to–

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States.;

(20) "protected computer" has the meaning set forth in section 1030; and

(21) "computer trespasser"--

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

§ 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who--

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when--

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or
(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b) to (c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use

that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with--

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this chapter.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any

criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in ~~this chapter or chapter 121~~ **this chapter or chapter 121 or 206 of this title** or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic ~~wire and oral~~ **wire, oral, and electronic** communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person--

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted--

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which--

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or
(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter--

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if–

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication--

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled, encrypted, or transmitted using modulation techniques the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication, then--

(i) if the communication is not the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, and the conduct is not that described in subsection (5), the offender shall be fined under this title or imprisoned not more than one year, or both; and

(ii) if the communication is the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, the offender shall be fined under this title.

(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted--

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)(a)(i) If the communication is--

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection--

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

§ 2516. Authorization for interception of wire, oral, or electronic communications

(1)The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of--
(a)any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 37 [18 USCS § § 791 et seq.] (relating to espionage), chapter 90 [18 USCS § § 1831 et seq.] (relating to protection of trade secrets), chapter 105 [18 USCS § § 2151 et seq.] (relating to sabotage), chapter 115 [18 USCS § § 2381 et seq.] (relating to treason), chapter 102 [18 USCS § § 2101 et seq.] (relating to riots), chapter 65 [18 USCS § § 1361 et seq.] (relating to malicious mischief), chapter 111 [18 USCS § § 2271 et seq.] (relating to destruction of vessels), or chapter 81 [18 USCS § § 1621 et seq.] (relating to piracy);
(b)a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves

murder, kidnapping, robbery, or extortion, and which is punishable under this title;
(c)any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 1014 (relating to loans and credit applications generally; renewals and discounts), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), sections 2251 and 2252 (sexual exploitation of children), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 38 (relating to aircraft parts fraud), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal official), ~~and section 1341 (relating to mail fraud),~~ **section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse),** or section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), section 1992 (relating to wrecking trains), a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), or section 1546 (relating to fraud and misuse of visas, permits, and other documents);
(d)any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;
(e)any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;
(f)any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g)a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions);
(h)any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;
(i)any felony violation of chapter 71 (relating to obscenity) of this title [18 USCS § § 1460 et seq.];
(j)any violation of section 60123(b) (relating to destruction of a natural gas pipeline) or 46502 (relating to aircraft piracy) of title 49;
(k)any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act);
(l)the location of any fugitive from justice from an offense described in this section;
(m)a violation of section 274, 277, or 278 of the Immigration and Nationality Act (8 U.S.C. 1324, 1327, or 1328) (relating to the smuggling of aliens);
(n)any felony violation of sections 922 and 924 of title 18, United States Code (relating to firearms);
(o)any violation of section 5861 of the Internal Revenue Code of 1986 [26 USCS § 5861] (relating to firearms); or
(p)a felony violation of section 1028 (relating to production of false identification documents), section 1542 (relating to false statements in passport applications), section 1546 (relating to fraud and misuse of visas, permits, and other documents) of this title or a violation of section 274, 277, or 278 of the Immigration and Nationality Act [8 USCS § 1324, 1327, or 1328] (relating to the smuggling of aliens); or
[(q)](p)any conspiracy to commit any offense described in any subparagraph of this paragraph.

(2)The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire, oral or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3)Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

§ 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

§ 2520. Recovery of civil damages authorized

(a) In general.--Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, ***other than the United States,*** which engaged in that violation such relief as may be appropriate.

(b) Relief.--In an action under this section, appropriate relief includes--

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of damages.--(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and not more than $500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1000.

(2) In any other action under this section, the court may assess as damages whichever is the greater of--

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

(d) Defense.--A good faith reliance on--

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other law.

(e) Limitation.--A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

(f) Administrative Discipline.– If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reason for such determination.

(g) Improper Disclosure is Violation.–Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for the purposes of section 2520(a).

TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I. CRIMES
CHAPTER 121. STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

~~§ 2702. Disclosure of contents~~ § 2702. Voluntary disclosure of customer communications or records

[N.B.: The table of contents for the section is amended to reflect the change in title.]

(a)Prohibitions. Except as provided in subsection (b)--
(1)a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
(2)a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--
(A)on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and
(B)solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.; and
(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

~~(b)Exceptions. A person or entity~~ **Exceptions for disclosure of communications.-- A provider described in subsection (a)** may divulge the contents of a communication--
(1)to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
(2)as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;
(3)with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
(4)to a person employed or authorized or whose facilities are used to forward such communication to its destination;
(5)as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or
(6)to a law enforcement agency--
(A)if the contents--
(i)were inadvertently obtained by the service provider; and
(ii)appear to pertain to the commission of a crime; or
(B)if required by section 227 of the Crime Control Act of 1990 [42 USCS § 13032]. ; **or**
(C) if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.

(c) Exceptions for disclosure of customer records.--A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or

(5) to any person other than a governmental entity.

~~§ 2703. Requirements for governmental access~~ **§ 2703. Required disclosure of customer communications or records**

[N.B.: The table of sections is also amended to reflect the change in title.]

~~(a)Contents of electronic~~ **Contents of wire or electronic** communications in electronic storage. A governmental entity may require the disclosure by a provider of electronic communication service of the ~~contents of an electronic~~ **contents of a wire or electronic** communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued ~~under the Federal Rules of Criminal Procedure~~ **using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation** or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the ~~contents of an electronic~~ **contents of a wire or electronic** communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.
(b)~~Contents of electronic~~ **Contents of wire or electronic** communications in a remote computing service.
(1)A governmental entity may require a provider of remote computing service to disclose the contents of ~~any electronic~~ **any wire or electronic** communication to which this paragraph is made applicable by paragraph (2) of this subsection--
(A)without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued ~~under the Federal Rules of Criminal Procedure~~ **using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation** or equivalent State warrant; or
(B)with prior notice from the governmental entity to the subscriber or customer if the governmental entity--
(i)uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
(ii)obtains a court order for such disclosure under subsection (d) of this section;
except that delayed notice may be given pursuant to section 2705 of this title.
(2)Paragraph (1) is applicable with respect to ~~any electronic~~ **any wire or electronic** communication that is held or maintained on that service--
(A)on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
(B)solely for the purpose of providing storage or computer processing services to such subscriber

or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c)Records concerning electronic communication service or remote computing service.
(1)(~~A)Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may~~ **A governmental entity may require a provider of electronic communication service or remote computing service to** disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)~~ covered by subsection (a) or (b) of this section) to any person other than a governmental entity.~~
~~(B)A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental entity--~~
~~(i)~~ **(A)** obtains a warrant issued under the Federal Rules of Criminal Procedure **using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation** or equivalent State warrant;
~~(ii)~~**(B)** obtains a court order for such disclosure under subsection (d) of this section;
~~(iii)~~**(C)** has the consent of the subscriber or customer to such disclosure; or
~~(iv)~~**(D)** submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title). **; or**

(E) seeks information under paragraph (2).

~~(C)~~ **(2)**A provider of electronic communication service or remote computing service shall disclose to a governmental ~~entity the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber~~ **entity the--**

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service ~~and the types of services the subscriber or customer utilized~~, when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under ~~subparagraph (B)~~ **paragraph (1).**
~~(2)~~**(3)** A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d)Requirements for court order. A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction ~~described in section 3127(2)(A)~~ and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e)No cause of action against a provider disclosing information under this chapter. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, or certification under this chapter [18 USCS § § 2701 et seq.].

(f)Requirement to preserve evidence.
(1)In general. A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.
(2)Period of retention. Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

§ 2707. Civil action

(a) Cause of action.--Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, ***other than the United States,*** which engaged in that violation such relief as may be appropriate.

(b) Relief.--In a civil action under this section, appropriate relief includes--

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages.--The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

~~(d) Disciplinary actions for violations.--If a court determines that any agency or department of the United States has violated this chapter and the court finds that the circumstances surrounding the violation raise the question whether or not an officer or employee of the agency or department acted willfully or intentionally with respect to the violation, the agency or department concerned shall promptly initiate a proceeding to determine whether or not disciplinary action is warranted against the officer or employee.~~
(d) Administrative Discipline.–If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the possible violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(e) Defense.--A good faith reliance on--

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization ***(including a request of a governmental entity under section 2703(f) of this title);***

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

(f) Limitation.--A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

(g) Improper Disclosure.–Any willful disclosure of a 'record', as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.

§ 2711. Definitions for chapter

As used in this chapter--

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.; and

(3) the term 'court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.

§ 2712. Civil actions against the United States.

[N.B.: The table of contents at the beginning of the chapter is amended to include this section.]

(a) In General.–Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 USC 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the court may assess as damages–

(1) actual damages, but not less than $10,000, whichever amount is greater; and

(2) litigation costs, reasonably incurred.

(b) Procedures.–

(1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.

(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.

(3) Any action under this section shall be tried to the court without a jury.

(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

(c) Administrative Discipline.–If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the possible violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(d) Exclusive Remedy.–Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

(e) Stay of Proceedings.–

(1) Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).

(2) In this subsection, the terms 'related criminal case' and 'related investigation' mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical.

(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party.

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART II--CRIMINAL PROCEDURE
CHAPTER 203--ARREST AND COMMITMENT

§ 3056. Powers, authorities, and duties of United States Secret Service

(a) Under the direction of the Secretary of the Treasury, the United States Secret Service is authorized to protect the following persons:

(1) The President, the Vice President (or other officer next in the order of succession to the Office of President), the President-elect, and the Vice President-elect.

(2) The immediate families of those individuals listed in paragraph (1).

(3) Former Presidents and their spouses for their lifetimes, except that protection of a spouse shall terminate in the event of remarriage unless the former President did not serve as President prior to January 1, 1997, in which case, former Presidents and their spouses for a period of not more than ten years from the date a former President leaves office, except that--

(A) protection of a spouse shall terminate in the event of remarriage or the divorce from, or death of a former President; and

(B) should the death of a President occur while in office or within one year after leaving office, the spouse shall receive protection for one year from the time of such death:

Provided, That the Secretary of the Treasury shall have the authority to direct the Secret Service to provide temporary protection for any of these individuals at any time if the Secretary of the Treasury or designee determines that information or conditions warrant such protection.

(4) Children of a former President who are under 16 years of age for a period not to exceed ten years or upon the child becoming 16 years of age, whichever comes first.

(5) Visiting heads of foreign states or foreign governments.

(6) Other distinguished foreign visitors to the United States and official representatives of the United States performing special missions abroad when the President directs that such protection be provided.

(7) Major Presidential and Vice Presidential candidates and, within 120 days of the general Presidential election, the spouses of such candidates. As used in this paragraph, the term "major Presidential and Vice Presidential candidates" means those individuals identified as such by the Secretary of the Treasury after consultation with an advisory committee consisting of the Speaker of the House of Representatives, the minority leader of the House of Representatives, the majority and minority leaders of the Senate, and one additional member selected by the other members of the committee.

The protection authorized in paragraphs (2) through (7) may be declined.

(b) Under the direction of the Secretary of the Treasury, the Secret Service is authorized to detect and arrest any person who violates--

(1) section 508, 509, 510, 871, or 879 of this title or, with respect to the Federal Deposit Insurance Corporation, Federal land banks, and Federal land bank associations, section 213, 216, 433, 493, 657, 709, 1006, 1007, 1011, 1013, 1014, 1907, or 1909 of this title;

(2) any of the laws of the United States relating to coins, obligations, and securities of the United States and of foreign governments; or

(3) any of the laws of the United States relating to electronic fund transfer frauds, ~~credit and debit card frauds, and false identification documents or devices~~ ***access device frauds, false identification documents or devices, and any fraud or other criminal or unlawful activity in or against any federally insured financial institution;*** except that the authority conferred by this paragraph shall be exercised subject to the agreement of the Attorney General and the Secretary of the Treasury and shall not affect the authority of any other Federal law enforcement agency with respect to those laws.

(c)(1) Under the direction of the Secretary of the Treasury, officers and agents of the Secret Service are authorized to--

(A) execute warrants issued under the laws of the United States;

(B) carry firearms;

(C) make arrests without warrant for any offense against the United States committed in their presence, or for any felony cognizable under the laws of the United States if they have reasonable grounds to believe that the person to be arrested has committed or is committing such felony;

(D) offer and pay rewards for services and information leading to the apprehension of persons involved in the violation or potential violation of those provisions of law which the Secret Service is authorized to enforce;

(E) pay expenses for unforeseen emergencies of a confidential nature under the direction of the Secretary of the Treasury and accounted for solely on the Secretary's certificate; and

(F) perform such other functions and duties as are authorized by law.

(2) Funds expended from appropriations available to the Secret Service for the purchase of counterfeits and subsequently recovered shall be reimbursed to the appropriations available to the Secret Service at the time of the reimbursement.

(d) Whoever knowingly and willfully obstructs, resists, or interferes with a Federal law enforcement agent engaged in the performance of the protective functions authorized by this section or by section 1752 of this title shall be fined not more than $1,000 or imprisoned not more than one year, or both.

(e)(1) When directed by the President, the United States Secret Service is authorized to participate, under the direction of the Secretary of the Treasury, in the planning, coordination, and implementation of security operations at special events of national significance, as determined by the President.

(2) At the end of each fiscal year, the President through such agency or office as the President may designate, shall report to the Congress--

(A) what events, if any, were designated special events of national significance for security purposes under paragraph (1); and

(B) the criteria and information used in making each designation.

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART II--CRIMINAL PROCEDURE

CHAPTER 204--REWARDS FOR INFORMATION CONCERNING TERRORIST ACTS AND ESPIONAGE

§ 3077. Definitions

As used in this chapter, the term--

~~(1) "act of terrorism" means an activity that--~~

~~(A) involves a violent act or an act dangerous to human life that is a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; and~~

~~(B) appears to be intended--~~

~~(i) to intimidate or coerce a civilian population;~~

~~(ii) to influence the policy of a government by intimidation or coercion; or~~

~~(iii) to affect the conduct of a government by assassination or kidnapping;~~

(1) "act of terrorism" means an act of domestic or international terrorism as defined in section 2331;

...

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART II--CRIMINAL PROCEDURE
CHAPTER 205--SEARCHES AND SEIZURES

§ 3103a. Additional grounds for issuing warrant

(a) In general.– In addition to the grounds for issuing a warrant in section 3103 of this title, a warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States.

(b) Delay.– With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if–

(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705);

(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and

(3) the warrant provides for the giving of such notice within a reasonable period of its execution, which period may thereafter be extended by the court for good cause shown.

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART II--CRIMINAL PROCEDURE
CHAPTER 206--PEN REGISTERS AND TRAP AND TRACE DEVICES

§ 3121. General prohibition on pen register and trap and trace device use; exception

(a)In general. Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b)Exception. The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service--
(1)relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or
(2)to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or
(3)where the consent of the user of that service has been obtained.

(c)Limitation. A government agency authorized to install and use a pen register **or trap and trace device** under this chapter [18 USCS § § 3121 et seq.] or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, **routing, addressing,** and signaling information utilized in ~~call processing~~ **the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.**

(d)Penalty. Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

§ 3123. Issuance of an order for a pen register or a trap and trace device

~~(a)In general. Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds that the attorney for the Government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.~~

(a) In general–

(1) Attorney for the government.– Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

(2) State investigative or law enforcement officer.– Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

(3)(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify–
(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;
(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;
(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and
(iv) any information which has been collected by the device.
To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.

(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).

(b)Contents of order. An order issued under this section--
(1)shall specify--
(A)the identity, if known, of the person to whom is leased or in whose name is listed the telephone line **or other facility** to which the pen register or trap and trace device is to be attached **or applied;**
(B)the identity, if known, of the person who is the subject of the criminal investigation;
~~(C)the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and~~
(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and
(D)a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and
(2)shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.

(c)Time period and extensions.
(1)An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.
(2)Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.

(d)Nondisclosure of existence of pen register or a trap and trace device. An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that--
(1)the order be sealed until otherwise ordered by the court; and
(2)the person owning or leasing the line **or other facility** to which the pen register or a trap and trace device is attached, ~~or who has been ordered by the court~~ **or applied, or who is obligated by the order** to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

§ 3124. Assistance in installation and use of a pen register or a trap and trace device

...

(b) Trap and trace device.--Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line ***or other facility*** and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a

minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 3123(b)(2) of this title. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished, pursuant to section 3123(b) or section 3125 of this title, to the officer of a law enforcement agency, designated in the
court order, at reasonable intervals during regular business hours for the duration of the order.

(d) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with ~~the terms of~~ a court order under this chapter or request pursuant to section 3125 of this title.

...

§ 3127. Definitions for chapter

As used in this chapter--

(1) the terms "wire communication", "electronic communication", ~~and~~ "electronic communication service", ***and "contents"*** have the meanings set forth for such terms in section 2510 of this title;

(2) the term "court of competent jurisdiction" means--

~~(A) a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals; or~~

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;

(3) the term "pen register" means a device ***or process*** which records or decodes ~~electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached~~ ***dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication,*** but such term does not include any device ***or process*** used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device ***or process*** used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

(4) the term "trap and trace device" means a device ***or process*** which captures the incoming electronic or other impulses which identify the originating number ~~of an instrument or device from which a wire or electronic communication was transmitted~~ ***or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;***

(5) the term "attorney for the Government" has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

(6) the term "State" means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART II--CRIMINAL PROCEDURE
CHAPTER 213--LIMITATIONS

~~§ 3286. Extension of statute of limitation for certain terrorism offenses~~

~~Notwithstanding section 3282, no person shall be prosecuted, tried, or punished for any non-capital offense involving a violation of section 32 (aircraft destruction), section 37 (airport violence), section 112 (assaults upon diplomats), section 351 (crimes against Congressmen or Cabinet officers), section 1116 (crimes against diplomats), section 1203 (hostage taking), section 1361 (willful injury to government property), section 1751 (crimes against the President), section 2280 (maritime violence), section 2281 (maritime platform violence), section 2332 (terrorist acts abroad against United States nationals), section 2332a (use of weapons of mass destruction), 2332b (acts of terrorism transcending national boundaries), or section 2340A (torture) of this title or section 46502, 46504, 46505, or 46506 of title 49, unless the indictment is found or the information is instituted within 8 years after the offense was committed.~~

§ 3286. Extension of statute of limitation for certain terrorism offenses

(a) Eight-year limitation.–Notwithstanding section 3282, no person shall be prosecuted, tried, or punished for any noncapital offense involving a violation of any provision listed in section 2332b(g)(5)(B), or a violation of section 112, 351(e), 1361, or 1751(e) of this title, or section 46504, 46505, or 46506 of title 49, unless the indictment is found or the information is instituted within 8 years after the offense was committed. Notwithstanding the preceding sentence, offenses listed in section 3295 are subject to the statute of limitations set forth in that section.

(b) No limitation.–Notwithstanding any other law, an indictment may be found or an information instituted at any time without limitation for any offense listed in section

2332b(g)(5)(B), if the commission of such offense resulted in, or created a foreseeable risk of, death or serious bodily injury to another person.

Sec. 809. No statute of limitation for certain terrorism offenses.

(b) Application.–The amendments made by this section shall apply to the prosecution of any offense committed before, on, or after the date of the enactment of this section.

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART II--CRIMINAL PROCEDURE
CHAPTER 227--SENTENCES
SUBCHAPTER D--IMPRISONMENT

§ 3583. Inclusion of a term of supervised release after imprisonment

(a) In general.--The court, in imposing a sentence to a term of imprisonment for a felony or a misdemeanor, may include as a part of the sentence a requirement that the defendant be placed on a term of supervised release after imprisonment, except that the court shall include as a part of the sentence a requirement that the defendant be placed on a term of supervised release if such a term is required by statute or if the defendant has been convicted for the first time of a domestic violence crime as defined in section 3561(b).

(b) Authorized terms of supervised release.--Except as otherwise provided, the authorized terms of supervised release are--

(1) for a Class A or Class B felony, not more than five years;

(2) for a Class C or Class D felony, not more than three years; and

(3) for a Class E felony, or for a misdemeanor (other than a petty offense), not more than one year.

...

(j) Supervised release terms for terrorism predicates.–Notwithstanding subsection (b), the authorized term of supervised release for any offense listed in section 2332b(g)(5)(B), the commission of which resulted in, or created a foreseeable risk of, death or serious bodily injury to another person, is any term of years or life.

UNITED STATES CODE ANNOTATED
TITLE 47. TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS
CHAPTER 5--WIRE OR RADIO COMMUNICATION
SUBCHAPTER V-A--CABLE COMMUNICATIONS
PART IV--MISCELLANEOUS PROVISIONS

Section 551. Protection of subscriber privacy

...

(c) Disclosure of personally identifiable information

(1) Except as provided in paragraph (2), a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator.

(2) A cable operator may disclose such information if the disclosure is--

(A) necessary to render, or conduct a legitimate business activity related to, a cable service or other service provided by the cable operator to the subscriber;

(B) subject to subsection (h) of this section, made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed; ~~or~~

(C) a disclosure of the names and addresses of subscribers to any cable service or other service, if--
(i) the cable operator has provided the subscriber the opportunity to prohibit or limit such disclosure, and
(ii) the disclosure does not reveal, directly or indirectly, the--
(I) extent of any viewing or other use by the subscriber of a cable service or other service provided by the cable operator, or
(II) the nature of any transaction made by the subscriber over the cable system of the cable operator.**; or**

(D) to a government entity as authorized under chapters 119, 121, or 206 of title 18, United States Code, except that such disclosure shall not include records revealing cable subscriber selection of video programming from a cable operator.

...

(h) Disclosure of information to governmental entity pursuant to court order

~~A governmental entity~~ **Except as provided in subsection (c)(2)(D), a governmental entity** may obtain personally identifiable information concerning a cable subscriber pursuant to a court order only if, in the court proceeding relevant to such court order–

(1) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and
(2) the subject of the information is afforded the opportunity to appear and contest such entity's claim.

UNITED STATES CODE ANNOTATED
FEDERAL RULES OF CRIMINAL PROCEDURE FOR THE UNITED STATES DISTRICT COURTS
III. INDICTMENT AND INFORMATION

Rule 6. The Grand Jury

...

(e) Recording and Disclosure of Proceedings.

(1) Recording of Proceedings. All proceedings, except when the grand jury is deliberating or voting, shall be recorded stenographically or by an electronic recording device. An unintentional failure of any recording to reproduce all or any portion of a proceeding shall not affect the validity of the prosecution. The recording or reporter's notes or any transcript prepared therefrom shall remain in the custody or control of the attorney for the government unless otherwise ordered by the court in a particular case.

(2) General Rule of Secrecy. A grand juror, an interpreter, a stenographer, an operator of a recording device, a typist who transcribes recorded testimony, an attorney for the government, or any person to whom disclosure is made under paragraph (3)(A)(ii) of this subdivision shall not disclose matters occurring before the grand jury, except as otherwise provided for in these rules. No obligation of secrecy may be imposed on any person except in accordance with this rule. A knowing violation of Rule 6 may be punished as a contempt of court.

(3) Exceptions.

(A) Disclosure otherwise prohibited by this rule of matters occurring before the grand jury, other than its deliberations and the vote of any grand juror, may be made to--

(i) an attorney for the government for use in the performance of such attorney's duty; and

(ii) such government personnel (including personnel of a state or subdivision of a state) as are deemed necessary by an attorney for the government to assist an attorney for the government in the performance of such attorney's duty to enforce federal criminal law.

(B) Any person to whom matters are disclosed under subparagraph (A)(ii) of this paragraph shall not utilize that grand jury material for any purpose other than assisting the attorney for the government in the performance of such attorney's duty to enforce federal criminal law. An attorney for the government shall promptly provide the district court, before which was impaneled the grand jury whose material has been so disclosed, with the names of the persons to whom such disclosure has been made, and shall certify that the attorney has advised such persons of their obligation of secrecy under this rule.

~~(C) Disclosure otherwise prohibited by this rule of matters occurring before the grand jury may also be made --~~

~~(i) when so directed by a court preliminarily to or in connection with a judicial proceeding;~~

~~(ii)when permitted by a court at the request of the defendant, upon a showing that grounds may exist for a motion to dismiss the indictment because of matters occurring before the grand jury;~~

~~(iii) when the disclosure is made by an attorney for the government to another federal grand jury; or~~

~~(iv) when permitted by a court at the request of an attorney for the government, upon a showing that such matters may disclose a violation of state criminal law, to an appropriate official of a state or subdivision of a state for the purpose of enforcing such law.~~

~~If the court orders disclosure of matters occurring before the grand jury, the disclosure shall be made in such manner, at such time, and under such conditions as the court may direct.~~

(C)(i) Disclosure otherwise prohibited by this rule of matters occurring before the grand jury may also be made--

(I) when so directed by a court preliminarily to or in connection with a judicial proceeding;

(II) when permitted by a court at the request of the defendant, upon a showing that grounds may exist for a motion to dismiss the indictment because of matters occurring before the grand jury;

(III) when the disclosure is made by an attorney for the government to another Federal grand jury;

(IV) when permitted by a court at the request of an attorney for the government, upon a showing that such matters may disclose a violation of state criminal law, to an appropriate official of a state or subdivision of a state for the purpose of enforcing such law; or

(V) when the matters involve foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in clause (iv) of this subparagraph), to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties.

(ii) If the court orders disclosure of matters occurring before the grand jury, the disclosure shall be made in such manner, at such time, and under such conditions as the court may direct.

(iii) Any Federal official who receives information pursuant to clause (i)(V) of this subparagraph may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information. Within a reasonable time after such disclosure, an attorney for the government shall file under seal a notice with the court stating the fact that such information was disclosed and the departments, agencies, or entities to which the disclosure was made.

(iv) In clause (i)(V) of this subparagraph, the term 'foreign intelligence information' means—

(I) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

(aa) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(bb) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(cc) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(II) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

(aa) the national defense or the security of the United States; or

(bb) the conduct of the foreign affairs of the United States.

(D) A petition for disclosure pursuant to subdivision (e)(3)(C)(i) (e)(3)(C)(i)(I) shall be filed in the district where the grand jury convened. Unless the hearing is ex parte, which it may be when the petitioner is the government, the petitioner shall serve written notice of the petition upon (i) the attorney for the government, (ii) the parties to the judicial proceeding if disclosure is sought in connection with such a proceeding, and (iii) such other persons as the court may direct. The court shall afford those persons a reasonable opportunity to appear and be heard.

(E) If the judicial proceeding giving rise to the petition is in a federal district court in another district, the court shall transfer the matter to that court unless it can reasonably obtain sufficient

knowledge of the proceeding to determine whether disclosure is proper. The court shall order transmitted to the court to which the matter is transferred the material sought to be disclosed, if feasible, and a written evaluation of the need for continued grand jury secrecy. The court to which the matter is transferred shall afford the aforementioned persons a reasonable opportunity to appear and be heard.

(4) Sealed Indictments. The federal magistrate judge to whom an indictment is returned may direct that the indictment be kept secret until the defendant is in custody or has been released pending trial. Thereupon the clerk shall seal the indictment and no person shall disclose the return of the indictment except when necessary for the issuance and execution of a warrant or summons.

(5) Closed Hearing. Subject to any right to an open hearing in contempt proceedings, the court shall order a hearing on matters affecting a grand jury proceeding to be closed to the extent necessary to prevent disclosure of matters occurring before a grand jury.

(6) Sealed Records. Records, orders and subpoenas relating to grand jury proceedings shall be kept under seal to the extent and for such time as is necessary to prevent disclosure of matters occurring before a grand jury.
...

PROVISIONS NOT AMENDING THE UNITED STATES CODE OR FEDERAL RULES OF CRIMINAL PROCEDURE

Sec. 105. Expansion of national electronic crime task force initiative.

The Director of the United States Secret Service shall take appropriate actions to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, throughout the United States, for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

Sec. 203. Authority to share criminal investigative information.

(c) Procedures.—The Attorney General shall establish procedures for the disclosure of information pursuant to section 2517(6) and Rule 6(e)(3)(C)(i)(V) of the Federal Rules of Criminal Procedure that identifies a United States person, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)).

(d) Foreign Intelligence Information.—

(1) In General.—Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information obtained as part of a criminal

investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(2) DEFINITION.—In this subsection, the term ''foreign intelligence information'' means—

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States.

Sec. 222. Assistance to Law Enforcement Agencies

Nothing in this Act shall impose any additional technical obligation or requirement on a provider of a wire or electronic communication service or other person to furnish facilities or technical assistance. A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to section 216 shall be reasonably compensated for such reasonable expenditures incurred in providing such facilities or assistance.

Sec. 224. Sunset.

(a) In General.–Except as provided in subsection (b), this title and the amendments made by this title (other than sections 203(a), 203(c), 205, 208, 210 211, 213, 216, 219, 221, and 222, and the amendments made by those sections) shall cease to have effect on December 31, 2005.

(b) Exception.–With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in subsection (a) cease to have effect, or

with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect.

Sec. 816. Development and support of cybersecurity forensic capabilities.

(a) In General.—The Attorney General shall establish such regional computer forensic laboratories as the Attorney General considers appropriate, and provide support to existing computer forensic laboratories, in order that all such computer forensic laboratories have the capability—

***(1) to provide forensic examinations with respect to seized or intercepted computer evidence re*lating to criminal activity (including cyberterrorism);**

(2) to provide training and education for Federal, State, and local law enforcement personnel and prosecutors regarding investigations, forensic analyses, and prosecutions of computer-related crime (including cyberterrorism);

(3) to assist Federal, State, and local law enforcement in enforcing Federal, State, and local criminal laws relating to computer-related crime;

(4) to facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer-related crime with State and local law enforcement personnel and prosecutors, including the use of multijurisdictional task forces; and

(5) to carry out such other activities as the Attorney General considers appropriate.

(b) Authorization of appropriations.—

(1) Authorization.—There is hereby authorized to be appropriated in each fiscal year $50,000,000 for purposes of carrying out this section.

(2) Availability.—Amounts appropriated pursuant to the authorization of appropriations in paragraph (1) shall remain available until expended.