# H.R. 3162 – The 2001 Anti-Terrorism Legislation

[Pub. L. No. 107-56 (Oct. 26, 2001)]

## Abridged – Provisions Relating to Obtaining Electronic Evidence and Others of Interest to State & Local Law Enforcers – With Section Summaries[1]

**SECTION 1. SHORT TITLE AND TABLE OF CONTENTS.**

(a) SHORT TITLE- This Act may be cited as the `Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001'.

(b) TABLE OF CONTENTS- The table of contents for this Act is as follows:



---

[1] The added section summaries were drawn in pertinent part from the *Field Guidance* … memorandum issued by the U.S. Department of Justice; otherwise from the "section-by-section analysis" of the bill found on the Web site of U.S. Senator Patrick Leahy (D., Vt.), http://www.senate.gov/~leahy/press/200110/102401a.html.

* * *

## TITLE I--ENHANCING DOMESTIC SECURITY AGAINST TERRORISM

* * *

**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.

SUMMARY: Both the House and Senate bills included this provision to allow the Secret Service to develop a national network of electronic crime task forces, based on the highly successful New York Electronic Crimes Task Force model, for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems. Not in original Administration proposal.

* * *

## TITLE II--ENHANCED SURVEILLANCE PROCEDURES

### SEC. 201. AUTHORITY TO INTERCEPT WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS RELATING TO TERRORISM.

Section 2516(1) of title 18, United States Code, is amended--

(1) by redesignating paragraph (p), as so redesignated by section 434(2) of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104-132; 110 Stat. 1274), as paragraph (r); and

(2) by inserting after paragraph (p), as so redesignated by section 201(3) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (division C of Public Law 104-208; 110 Stat. 3009-565), the following new paragraph:

`(q) any criminal violation of section 229 (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2339A, or 2339B of this title (relating to terrorism); or'.

SUMMARY: Both the House and Senate bills included this provision to add criminal violations relating to terrorism to the list of predicate statutes in the criminal procedures for interception of communications under chapter 119 of title 18, United States Code. Not in original Administration proposal.

### SEC. 202. AUTHORITY TO INTERCEPT WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS RELATING TO COMPUTER FRAUD AND ABUSE OFFENSES.

Section 2516(1)(c) of title 18, United States Code, is amended by striking `and section 1341 (relating to mail fraud),' and inserting `section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse),'.

SUMMARY: Under previous law, investigators could not obtain a wiretap order to intercept *wire* communications (those involving the human voice) for violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030). For example, in several investigations, hackers have stolen teleconferencing services from a telephone company and used this mode of communication to plan and execute hacking attacks.

*Amendment:* Section 202 amends 18 U.S.C. § 2516(1) – the subsection that lists those crimes for which investigators may obtain a wiretap order for wire communications – by adding felony violations of 18 U.S.C. § 1030 to the list of predicate offenses.[2] This provision will sunset December 31, 2005.

### SEC. 203. AUTHORITY TO SHARE CRIMINAL INVESTIGATIVE INFORMATION.

(a) AUTHORITY TO SHARE GRAND JURY INFORMATION-

(1) IN GENERAL- Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure is amended to read as follows:

`(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.

---

[2] This amendment does not affect applications to intercept *electronic* communications in hacking investigations. As before, investigators may base an application to intercept electronic communications on any federal felony criminal violation. 18 U.S.C. § 2516(3).

`(iii) Any Federal official to whom information is disclosed 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 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.'.

(2) CONFORMING AMENDMENT- Rule 6(e)(3)(D) of the Federal Rules of Criminal Procedure is amended by striking `(e)(3)(C)(i)' and inserting `(e)(3)(C)(i)(I)'.

(b) AUTHORITY TO SHARE ELECTRONIC, WIRE, AND ORAL INTERCEPTION INFORMATION-

(1) LAW ENFORCEMENT- Section 2517 of title 18, United States Code, is amended by inserting at the end the following:

`(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.'.

(2) DEFINITION- Section 2510 of title 18, United States Code, is amended by--

(A) in paragraph (17), by striking `and' after the semicolon;

(B) in paragraph (18), by striking the period and inserting `; and'; and

(C) by inserting at the end the following:

`(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.'.

(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.

SUMMARY: Both the House and Senate bills included provisions amending the criminal procedures for interception of communications under chapter 119 of title 18, United States Code, and the grand jury procedures under Rule 6(e) of the Federal Rules of Criminal Procedures to authorize disclosure of foreign intelligence information obtained by such interception or by a grand jury to any Federal law enforcement, intelligence, national security, national defense, protective or immigration personnel to assist the official receiving that information in the performance of his official duties. Section 203(a) requires that within a reasonable time after disclosure of any grand jury information, an attorney for the government notify the court of such disclosure and the departments, agencies or entities to which disclosure was made. Section 203(b) pertains to foreign intelligence information obtained by intercepting communications pursuant to a court-ordered wiretap. Section 203(c) also authorizes such disclosure of information obtained as part of a criminal investigation notwithstanding any other law.

The information must meet statutory definitions of foreign intelligence or counterintelligence or foreign intelligence information. Recipients may use that information only as necessary for their official duties, and use of the information outside those limits remains subject to applicable penalties, such as penalties for unauthorized disclosure under chapter 119, contempt penalties under Rule 6(e) and the Privacy Act. The Attorney General must establish procedures for disclosure of information that identifies a United States person, such as the current procedures established under Executive Order 12333 for the intelligence community. Modified Administration proposal to limit scope of personnel eligible to receive information. In case of grand jury information, limited proposal to require notification to court after disclosure.

**SEC. 204. CLARIFICATION OF INTELLIGENCE EXCEPTIONS FROM LIMITATIONS ON INTERCEPTION AND DISCLOSURE OF WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS.**

Section 2511(2)(f) of title 18, United States Code, is amended--

(1) by striking `this chapter or chapter 121' and inserting `this chapter or chapter 121 or 206 of this title'; and

(2) by striking `wire and oral' and inserting `wire, oral, and electronic'.

SUMMARY: Both the House and Senate bills included this provision to amend the criminal procedures for interception of wire, oral, and electronic communications in title 18, United States Code, to make clear that these procedures do not apply to the collection of foreign intelligence information under the statutory foreign intelligence authorities. Not in original Administration proposal.

* * *

**SEC. 209. SEIZURE OF VOICE-MAIL MESSAGES PURSUANT TO WARRANTS.**

Title 18, United States Code, is amended--

(1) in section 2510--

(A) in paragraph (1), by striking beginning with `and such' and all that follows through `communication'; and

(B) in paragraph (14), by inserting `wire or' after `transmission of'; and

(2) in subsections (a) and (b) of section 2703--

(A) by striking `CONTENTS OF ELECTRONIC' and inserting `CONTENTS OF WIRE OR

ELECTRONIC' each place it appears;
(B) by striking `contents of an electronic' and inserting `contents of a wire or electronic' each place it appears; and
(C) by striking `any electronic' and inserting `any wire or electronic' each place it appears.

SUMMARY: Under previous law, the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2703 *et seq.*, governed law enforcement access to stored electronic communications (such as e-mail), but not stored wire communications (such as voice-mail). Instead, the wiretap statute governed such access because the definition of "wire communication" (18 U.S.C. § 2510(1)) included stored communications, arguably requiring law enforcement to use a wiretap order (rather than a search warrant) to obtain unopened voice communications. Thus, law enforcement authorities used a wiretap order to obtain voice communications stored with a third party provider but could use a search warrant if that same information were stored on an answering machine inside a criminal's home.

Regulating stored wire communications through section 2510(1) created large and unnecessary burdens for criminal investigations. Stored voice communications possess few of the sensitivities associated with the real-time interception of telephones, making the extremely burdensome process of obtaining a wiretap order unreasonable.

Moreover, in large part, the statutory framework envisions a world in which technology-mediated voice communications (such as telephone calls) are conceptually distinct from non-voice communications (such as faxes, pager messages, and e-mail). To the limited extent that Congress acknowledged that data and voice might co-exist in a single transaction, it did not anticipate the convergence of these two kinds of communications typical of today's telecommunications networks. With the advent of MIME — Multipurpose Internet Mail Extensions — and similar features, an e-mail may include one or more "attachments" consisting of any type of data, including voice recordings. As a result, a law enforcement officer seeking to obtain a suspect's unopened e-mail from an ISP by means of a search warrant (as required under 18 U.S.C. § 2703(a)) had no way of knowing whether the inbox messages include voice attachments (*i.e.*, wire communications) which could not be compelled using a search warrant.

*Amendment:* Section 209 of the Act alters the way in which the wiretap statute and ECPA apply to stored voice communications.[3] The amendments delete "electronic storage" of wire communications from the definition of "wire communication" in section 2510 and insert language in section 2703 to ensure that stored wire communications are covered under the same rules as stored electronic communications. Thus, law enforcement can now obtain such communications using the procedures set out in section 2703 (such as a search warrant), rather than those in the wiretap statute (such as a wiretap order).

This provision will sunset December 31, 2005.

**SEC. 210. SCOPE OF SUBPOENAS FOR RECORDS OF ELECTRONIC COMMUNICATIONS.**

Section 2703(c)(2) of title 18, United States Code, as redesignated by section 212, is amended--
(1) by striking `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' and inserting the following: `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'; and
(2) by striking `and the types of services the subscriber or customer utilized,'.

[3] Note that these changes do not apply to voice messages in the possession of the user, such as the answering machine tape in a person's home. Those types of records remain outside of the statute.

SUMMARY: Subsection 2703(c) allows the government to use a subpoena to compel a limited class of information, such as the customer's name, address, length of service, and means of payment. Prior to the amendments in Section 210 of the Act, however, the list of records that investigators could obtain with a subpoena did not include certain records (such as credit card number or other form of payment for the communication service) relevant to determining a customer's true identity. In many cases, users register with Internet service providers using false names. In order to hold these individuals responsible for criminal acts committed online, the method of payment is an essential means of determining true identity.

Moreover, many of the definitions in section 2703(c) were technology-specific, relating primarily to telephone communications. For example, the list included "local and long distance telephone toll billing records," but did not include parallel terms for communications on computer networks, such as "records of session times and durations." Similarly, the previous list allowed the government to use a subpoena to obtain the customer's "telephone number or other subscriber number or identity," but did not define what that phrase meant in the context of Internet communications.

*Amendment:* Amendments to section 2703(c) update and expand the narrow list of records that law enforcement authorities may obtain with a subpoena. The new subsection 2703(c)(2) includes "records of session times and durations," as well as "any temporarily assigned network address." In the Internet context, such records include the Internet Protocol (IP) address assigned by the provider to the customer or subscriber for a particular session, as well as the remote IP address from which a customer connects to the provider. Obtaining such records will make the process of identifying computer criminals and tracing their Internet communications faster and easier.

Moreover, the amendments clarify that investigators may use a subpoena to obtain the "means and source of payment" that a customer uses to pay for his or her account with a communications provider, "including any credit card or bank account number." 18 U.S.C. §2703(c)(2)(F). While generally helpful, this information will prove particularly valuable in identifying the users of Internet services where a company does not verify its users' biographical information. (This section is not subject to the sunset provision in section 224 of the Act).

**SEC. 211. CLARIFICATION OF SCOPE.**

Section 631 of the Communications Act of 1934 (47 U.S.C. 551) is amended--

(1) in subsection (c)(2)--

(A) in subparagraph (B), by striking `or';

(B) in subparagraph (C), by striking the period at the end and inserting `; or'; and

(C) by inserting at the end the following:

`(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.'; and

(2) in subsection (h), by striking `A governmental entity' and inserting `Except as provided in subsection (c)(2)(D), a governmental entity'.

SUMMARY: The law contains two different sets of rules regarding privacy protection of communications and their disclosure to law enforcement: one governing cable service (the "Cable Act") (47 U.S.C. § 551), and the other applying to the use of telephone service and Internet access (the wiretap statute, 18 U.S.C. § 2510 et seq.; ECPA, 18 U.S.C. § 2701 et seq.; and the pen register and trap and trace statute (the "pen/trap" statute), 18 U.S.C. § 3121 et seq.).

Prior to the amendments in Section 211 of the Act, the Cable Act set out an extremely restrictive system of rules governing law enforcement access to most records possessed by a cable company. For example, the Cable Act did not allow the use of subpoenas or even search warrants to obtain such records. Instead, the cable company had to provide prior notice to the customer (even if he or she were the target of the investigation), and the government had to allow the customer to appear in court with an attorney and then justify to the court the investigative need to obtain the records. The court could then order disclosure of the records only if it found by "clear and convincing evidence" – a standard greater than probable cause or even a preponderance of the evidence – that the subscriber was "reasonably suspected" of engaging in criminal activity. This procedure was completely unworkable for virtually any criminal investigation.

The legal regime created by the Cable Act caused grave difficulties in criminal investigations because today, unlike in 1984 when Congress passed the Cable Act, many cable companies offer not only traditional cable programming services but also Internet access and telephone service. In recent years, some cable companies have refused to accept subpoenas and court orders pursuant to the pen/trap statute and ECPA, noting the seeming inconsistency of these statutes with the Cable

Act's harsh restrictions. See In re Application of United States, 36 F. Supp. 2d 430 (D. Mass. Feb. 9, 1999) (noting apparent statutory conflict and ultimately granting application for order under 18 U.S.C. 2703(d) for records from cable company providing Internet service). Treating identical records differently depending on the technology used to access the Internet made little sense. Moreover, these complications at times delayed or ended important investigations.

*Amendment:* Section 211 of the Act amends title 47, section 551(c)(2)(D), to clarify that ECPA, the wiretap statute, and the trap and trace statute govern disclosures by cable companies that relate to the provision of communication services – such as telephone and Internet services. The amendment preserves, however, the Cable Act's primacy with respect to records revealing what ordinary cable television programing a customer chooses to purchase, such as particular premium channels or "pay per view" shows. Thus, in a case where a customer receives both Internet access and conventional cable television service from a single cable provider, a government entity can use legal process under ECPA to compel the provider to disclose only those customer records relating to Internet service. (This section is not subject to the sunset provision in Section 224 of the Act).

**SEC. 212. EMERGENCY DISCLOSURE OF ELECTRONIC COMMUNICATIONS TO PROTECT LIFE AND LIMB.**

(a) DISCLOSURE OF CONTENTS-

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

(A) by striking the section heading and inserting the following:

`Sec. 2702. Voluntary disclosure of customer communications or records';

(B) in subsection (a)--

(i) in paragraph (2)(A), by striking `and' at the end;

(ii) in paragraph (2)(B), by striking the period and inserting `; and'; and

(iii) by inserting after paragraph (2) the following:

`(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.';

(C) in subsection (b), by striking `EXCEPTIONS- A person or entity' and inserting `EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS- A provider described in subsection (a)';

(D) in subsection (b)(6)--

(i) in subparagraph (A)(ii), by striking `or';

(ii) in subparagraph (B), by striking the period and inserting `; or'; and

(iii) by adding after subparagraph (B) the following:

`(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.'; and

(E) by inserting after subsection (b) the following:

`(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.'.

(2) TECHNICAL AND CONFORMING AMENDMENT- The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2702 and inserting the following:

`2702. Voluntary disclosure of customer communications or records.'.

(b) REQUIREMENTS FOR GOVERNMENT ACCESS-

(1) IN GENERAL- Section 2703 of title 18, United States Code, is amended--

(A) by striking the section heading and inserting the following:

`Sec. 2703. Required disclosure of customer communications or records';

(B) in subsection (c) by redesignating paragraph (2) as paragraph (3);

(C) in subsection (c)(1)--

(i) by striking `(A) Except as provided in subparagraph (B), a provider of electronic communication

service or remote computing service may' and inserting `A governmental entity may require a provider of electronic communication service or remote computing service to';
(ii) by striking `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' and inserting `)';
(iii) by redesignating subparagraph (C) as paragraph (2);
(iv) by redesignating clauses (i), (ii), (iii), and (iv) as subparagraphs (A), (B), (C), and (D), respectively;
(v) in subparagraph (D) (as redesignated) by striking the period and inserting `; or'; and
(vi) by inserting after subparagraph (D) (as redesignated) the following:
`(E) seeks information under paragraph (2).'; and
(D) in paragraph (2) (as redesignated) by striking `subparagraph (B)' and insert `paragraph (1)'.
(2) TECHNICAL AND CONFORMING AMENDMENT- The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2703 and inserting the following:
`2703. Required disclosure of customer communications or records.'.

SUMMARY: Previous law relating to voluntary disclosures by communication service providers was inadequate in two respects. *First*, it contained no special provision allowing providers to disclose customer records or communications in emergencies. If, for example, an Internet service provider ("ISP") independently learned that one of its customers was part of a conspiracy to commit an imminent terrorist attack, prompt disclosure of the account information to law enforcement could save lives. Since providing this information did not fall within one of the statutory exceptions, however, an ISP making such a disclosure could be sued civilly.

*Second*, prior to the Act, the law did not expressly permit a provider to voluntarily disclose *non-content* records (such as a subscriber's login records) to law enforcement for purposes of self-protection, even though providers could disclose the content of communications for this reason. See 18 U.S.C. § 2702(b)(5), 2703(c)(1)(B). Yet the right to disclose the content of communications necessarily implies the less intrusive ability to disclose non-content records. Cf. United States v. Auler, 539 F.2d 642, 646 n.9 (7th Cir. 1976) (phone company's authority to monitor and disclose conversations to protect against fraud necessarily implies right to commit lesser invasion of using, and disclosing fruits of, pen register device) (citing United States v. Freeman, 524 F.2d 337, 341 (7th Cir. 1975)). Moreover, as a practical matter, providers must have the right to disclose to law enforcement the facts surrounding attacks on their systems. For example, when an ISP's customer hacks into the ISP's network, gains complete control over an e-mail server, and reads or modifies the e-mail of other customers, the provider must have the legal ability to report the complete details of the crime to law enforcement.

*Amendment:* Section 212 corrects both of these inadequacies in previous law. Section 212 amends subsection 2702(b)(6) to permit, but not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure, however, does not create an affirmative obligation to review customer communications in search of such imminent dangers.

The amendments in Section 212 of the Act also change ECPA to allow providers to disclose information to protect their rights and property. It accomplishes this change by two related sets of amendments. First, amendments to sections 2702 and 2703 of title 18 simplify the treatment of voluntary disclosures by providers by moving all such provisions to 2702. Thus, section 2702 now regulates all permissive disclosures (of content and non-content records alike), while section 2703 covers only compulsory disclosures by providers. Second, an amendment to new subsection 2702(c)(3) clarifies that service providers *do* have the statutory authority to disclose non-content records to protect their rights and property. All of these changes will sunset December 31, 2005.

**SEC. 213. AUTHORITY FOR DELAYING NOTICE OF THE EXECUTION OF A WARRANT.**
Section 3103a of title 18, United States Code, is amended--
(1) by inserting `(a) IN GENERAL- ' before `In addition'; and
(2) by adding at the end the following:
`(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.'.

SUMMARY: Prior law governing the delayed provision of notice that a warrant had been executed was a mix of inconsistent rules, practices, and court decisions varying widely from jurisdiction to jurisdiction across the country. The lack of uniformity hindered the investigation of terrorism cases and other nationwide investigations.

Section 213 resolved this problem by amending 18 U.S.C. § 3103a to create a uniform statutory standard authorizing courts to delay the provision of required notice if the court finds "reasonable cause" to believe that providing immediate notification of the execution of the warrant may have an adverse result as defined by 18 U.S.C. § 2705 (including endangering the life or physical safety of an individual, flight from prosecution, evidence tampering, witness intimidation, or otherwise seriously jeopardizing an investigation or unduly delaying a trial). The section provides for the giving of notice within a "reasonable period" of a warrant's execution, which period can be further extended by a court for good cause.

This section is primarily designed to authorize delayed notice of *searches*, rather than delayed notice of *seizures*: the provision requires that any warrant issued under it must prohibit the seizure of any tangible property, any wire or electronic communication, or, except as expressly provided in chapter 121, any stored wire or electronic information, unless the court finds "reasonable necessity" for the seizure.

The "reasonable cause" standard adopted by the provision is in accord with prevailing caselaw for delayed notice of warrants. *See United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990) (government must show "good reason" for delayed notice of warrants). It is also in accord with the standards for exceptions to the general requirements that agents knock and announce themselves before entering and that warrants be executed during the daytime. *See Richards v. Wisconsin*, 520 U.S. 385 (1997) (no-knock entry to execute warrant is justified when the police have "reasonable suspicion" that knocking and announcing their presence would be dangerous or futile or would inhibit the effective investigation); Fed. R. Crim. P. 41(c)(1) ("The warrant shall be served in the daytime unless the issuing authority, by appropriate provision of the warrants, and for reasonable cause shown, authorizes its execution at times other than daytime.").

The requirement of notice within a "reasonable period" is a flexible standard to meet the circumstances of the case. *Villegas*, 899 F.2d at 1337 ("What constitutes a reasonable time will depend on the circumstances of each individual case"). Analogy to other statutes suggest that the period of delay could be substantial if circumstances warrant. *See* 18 U.S.C. § 2518(8)(d) (notice of a wiretap may be delayed for "a reasonable time" but not more than 90 days after the termination of the wiretap); *cf. United States v. Allie*, 978 F.2d 1401, 1405 (5th Cir. 1992) (suggesting that 60 days is a "reasonable period" for purposes of detaining a material witness under 18 U.S.C. § 3144). Caselaw regarding a "reasonable" period for delayed notice of warrants is still developing. The Second Circuit has interpreted it to ordinarily mean a seven-day initial delay, although subject to additional extensions. *Villegas*, 899 F.2d at 1337. The Ninth Circuit, although relying on the argument that the Constitution itself required prompt notice (*but see United States v. Pangburn*, 983 F.2d 449, 454-455 (2d Cir.1993); *Simons*, 206 F.3d 392, 403 (4th Cir. 2000) (45-day delay in notice of execution of warrant does not render search unconstitutional)), also has held that delays ordinarily should not exceed seven days. *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) ("Such time should not exceed seven days except upon a strong showing of necessity."). Other courts have suggested that a "reasonable period" could be significantly longer. *Cf. Simons*, 206 F.3d 392, 403 (45-day delay in notice of execution of search warrant did not render search unconstitutional).

The "reasonable necessity" standard for seizing items during the search is not well developed in the caselaw. The Second Circuit and other courts have equated the phrase "reasonable necessity" with "good reason" in the context of delayed notice. *Villegas*, 899 F.2d at 1337; *United States v. Ludwig*, 902 F. Supp 121, 126 (W.D. Tex. 1995); *accord United States v. Ibarra*, 725 F. Supp. 1195, 1200 (D. Wyo. 1989) ("reasonable necessity" to impound a vehicle).

In the weeks ahead, the Department may be providing additional guidance with respect to the use of this delayed notice provision. The Department expects that delayed notice will continue to be an infrequent exception to the general rule that notice of the execution of a warrant will be provided promptly.

* * *

**SEC. 216. MODIFICATION OF AUTHORITIES RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES.**

(a) GENERAL LIMITATIONS- Section 3121(c) of title 18, United States Code, is amended--

(1) by inserting `or trap and trace device' after `pen register';

(2) by inserting `, routing, addressing,' after `dialing'; and

(3) by striking `call processing' and inserting `the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications'.

(b) ISSUANCE OF ORDERS-

(1) IN GENERAL- Section 3123(a) of title 18, United States Code, is amended to read as follows:

`(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).'.

(2) CONTENTS OF ORDER- Section 3123(b)(1) of title 18, United States Code, is amended--

(A) in subparagraph (A)--

(i) by inserting `or other facility' after `telephone line'; and

(ii) by inserting before the semicolon at the end `or applied'; and

(B) by striking subparagraph (C) and inserting the following:

`(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'.

(3) NONDISCLOSURE REQUIREMENTS- Section 3123(d)(2) of title 18, United States Code, is amended--

(A) by inserting `or other facility' after `the line'; and
(B) by striking `, or who has been ordered by the court' and inserting `or applied, or who is obligated by the order'.

(c) DEFINITIONS-

(1) COURT OF COMPETENT JURISDICTION- Section 3127(2) of title 18, United States Code, is amended by striking subparagraph (A) and inserting the following:
`(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'.

(2) PEN REGISTER- Section 3127(3) of title 18, United States Code, is amended--
(A) by striking `electronic or other impulses' and all that follows through `is attached' and inserting `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'; and
(B) by inserting `or process' after `device' each place it appears.

(3) TRAP AND TRACE DEVICE- Section 3127(4) of title 18, United States Code, is amended--
(A) by striking `of an instrument' and all that follows through the semicolon and inserting `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;'; and
(B) by inserting `or process' after `a device'.

(4) CONFORMING AMENDMENT- Section 3127(1) of title 18, United States Code, is amended--
(A) by striking `and'; and
(B) by inserting `, and `contents' after `electronic communication service'.

(5) TECHNICAL AMENDMENT- Section 3124(d) of title 18, United States Code, is amended by striking `the terms of'.

(6) CONFORMING AMENDMENT- Section 3124(b) of title 18, United States Code, is amended by inserting `or other facility' after `the appropriate line'.

SUMMARY: The pen register and trap and trace statute (the "pen/trap" statute) governs the prospective collection of non-content traffic information associated with communications, such as the phone numbers dialed by a particular telephone. Section 216 updates the pen/trap statute in three important ways: (1) the amendments clarify that law enforcement may use pen/trap orders to trace communications on the Internet and other computer networks; (2) pen/trap orders issued by federal courts now have nationwide effect; and (3) law enforcement authorities must file a special report with the court whenever they use a pen/trap order to install their own monitoring device (such as the FBI's DCS1000) on computers belonging to a public provider. The following sections discuss these provisions in greater detail. (This section is not subject to the sunset provision in Section 224 of the Act).

Using pen/trap orders to trace communications on computer networks

When Congress enacted the pen/trap statute in 1986, it could not anticipate the dramatic expansion in electronic communications that would occur in the following fifteen years. Thus, the statute contained certain language that appeared to apply to telephone communications and that did not unambiguously encompass communications over computer networks.[4] Although numerous courts across the country have applied the pen/trap statue to communications on computer networks, no federal district or appellate court has explicitly ruled on its propriety. Moreover, certain private litigants have challenged the application of the pen/trap statute to such electronic communications based on the statute's telephone-specific language.

*Amendment:* Section 216 of the Act amends sections 3121, 3123, 3124, and 3127 of title 18 to clarify that the pen/trap statute applies to a broad variety of communications technologies. References to the target "line," for example, are revised to encompass a "line or other facility." Such a facility might include, for example, a cellular telephone number; a specific cellular telephone identified by its electronic serial number; an Internet user account or e-mail address; or an Internet

[4] For example, the statute defined "pen register" as "a device 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*." 18 U.S.C. § 3127(3) (emphasis supplied).

Protocol address, port number, or similar computer network address or range of addresses. In addition, because the statute takes into account a wide variety of such facilities, amendments to section 3123(b)(1)(C) now allow applicants for pen/trap orders to submit a description of the communications to be traced using any of these or other identifiers.

Moreover, the amendments clarify that orders for the installation of pen register and trap and trace devices may obtain any non-content information – all "dialing, routing, addressing, and signaling information" – utilized in the processing and transmitting of wire and electronic communications. Such information includes IP addresses and port numbers, as well as the "To" and "From" information contained in an e-mail header. Pen/trap orders cannot, however, authorize the interception of the content of a communication, such as words in the "subject line" or the body of an e-mail. Agents and prosecutors with questions about whether a particular type of information constitutes content should contact the Office of Enforcement Operations in the telephone context (202-514-6809) or the Computer Crime and Intellectual Property Section in the computer context (202-514-1026).

Further, because the pen register or trap and trace "device" often cannot be physically "attached" to the target facility, Section 216 makes two other related changes. First, in recognition of the fact that such functions are commonly performed today by software instead of physical mechanisms, the amended statute allows the pen register or trap and trace device to be "attached or applied" to the target facility. Likewise, Section 216 revises the definitions of "pen register" and "trap and trace device" in section 3127 to include an intangible "process" (such as a software routine) which collects the same information as a physical device.

Nationwide effect of pen/trap orders

Under previous law, a court could only authorize the installation of a pen/trap device "within the jurisdiction of the court." Because of deregulation in the telecommunications industry, however, a single communication may be carried by many providers. For example, a telephone call may be carried by a competitive local exchange carrier, which passes it to a local Bell Operating Company, which passes it to a long distance carrier, which hands it to a local exchange carrier elsewhere in the U.S., which in turn may finally hand it to a cellular carrier. If these carriers do not pass source information with each call, identifying that source may require compelling information from a string of providers located throughout the country – each requiring a separate order.

Moreover, since, under previous law, a court could only authorize the installation of a pen/trap device within its own jurisdiction, when one provider indicated that the source of a communication was a different carrier in another district, a second order in the new district became necessary. This order had to be acquired by a supporting prosecutor in the new district from a local federal judge – neither of whom had any other interest in the case. Indeed, in one case investigators needed three separate orders to trace a hacker's communications. This duplicative process of obtaining a separate order for each link in the communications chain has delayed or — given the difficulty of real-time tracing — completely thwarted important investigations.

*Amendment:* Section 216 of the Act divides section 3123 of title 18 into two separate provisions. New subsection (a)(1) gives federal courts the authority to compel assistance from any provider of communication services in the United States whose assistance is appropriate to effectuate the order.

For example, a federal prosecutor may obtain an order to trace calls made to a telephone within the prosecutor's local district. The order applies not only to the local carrier serving that line, but also to other providers (such as long-distance carriers and regional carriers in other parts of the country) through whom calls are placed to the target telephone. In some circumstances, the investigators may have to serve the order on the first carrier in the chain and receive from that carrier information identifying the communication's path to convey to the next carrier in the chain. The investigator would then serve the same court order on the next carrier, including the additional relevant connection information learned from the first carrier; the second carrier would then provide the connection information in its possession for the communication. The investigator would repeat this process until the order has been served on the originating carrier who is able to identify the source of the communication.

When prosecutors apply for a pen/trap order using this procedure, they generally will not know the name of the second or subsequent providers in the chain of communication covered by the order. Thus, the application and order will not necessarily name these providers. The amendments to section 3123 therefore specify that, if a provider requests it, law enforcement must provide a "written or electronic certification" that the order applies to that provider.

The amendments in Section 216 of the Act also empower courts to authorize the installation and use of pen/trap devices in other districts. Thus, for example, if a terrorism or other criminal investigation based in Virginia uncovers a conspirator using a phone or an Internet account in New York, the Virginia court can compel communications providers in New York to assist investigators in collecting information under a Virginia pen/trap order.

Consistent with the change above, Section 216 of the Act modifies section 3123(b)(1)(C) of title 18 to eliminate the requirement that federal pen/trap orders specify their geographic limits. However, because the new law gives nationwide effect for federal pen/trap orders, an amendment to section 3127(2)(A) imposes a "nexus" requirement: the issuing court must have jurisdiction over the particular crime under investigation.

Reports for use of law enforcement pen/trap devices on computer networks

Section 216 of the Act also contains an additional requirement for the use of pen/trap devices in a narrow class of cases. Generally, when law enforcement serves a pen/trap order on a communication service provider that provides Internet access or other computing services to the public, the provider itself should be able to collect the needed information and provide it to law enforcement. In certain rare cases, however, the provider may be unable to carry out the court order, necessitating installation of a device (such as Etherpeek or the FBI's DCS1000) to collect the information. In these infrequent cases, the amendments in section 216 require the law enforcement agency to provide the following information to the court under seal within thirty days: (1) the identity of the officers who installed or accessed the device; (2) the date and time the device was installed, accessed, and uninstalled; (3) the configuration of the device at installation and any modifications to that configuration; and (4) the information collected by the device. 18 U.S.C. § 3123(a)(3).

**SEC. 217. INTERCEPTION OF COMPUTER TRESPASSER COMMUNICATIONS.**

Chapter 119 of title 18, United States Code, is amended--

(1) in section 2510--

(A) in paragraph (18), by striking `and' at the end;

(B) in paragraph (19), by striking the period and inserting a semicolon; and

(C) by inserting after paragraph (19) the following:

`(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.'; and

(2) in section 2511(2), by inserting at the end the following:

`(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.'.

SUMMARY: Although the wiretap statute allows computer owners to monitor the activity on their machines to protect their rights and property, until Section 217 of the Act was enacted it was unclear whether computer owners could obtain the assistance of law enforcement in conducting such monitoring. This lack of clarity prevented law enforcement from assisting victims to take the natural and reasonable steps in their own defense that would be entirely legal in the physical world. In the physical world, burglary victims may invite the police into their homes to help them catch burglars in the act of committing their crimes. The wiretap statute should not block investigators from responding to similar requests in the computer context simply because the means of committing the burglary happen to fall within the definition of a "wire or electronic communication" according to the wiretap statute. Indeed, because providers often lack the expertise, equipment, or financial resources required to monitor attacks themselves, they commonly have no effective way to exercise their rights to protect

themselves from unauthorized attackers. This anomaly in the law created, as one commentator has noted, a "bizarre result," in which a "computer hacker's undeserved statutory privacy right trumps the legitimate privacy rights of the hacker's victims." Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 Wash. & Lee L. Rev. 1287, 1300 (2000).

*Amendment:* To correct this problem, the amendments in Section 217 of the Act allow victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems. Under new section 2511(2)(i), law enforcement may intercept the communications of a computer trespasser transmitted to, through, or from a protected computer. Before monitoring can occur, however, four requirements must be met. First, section 2511(2)(i)(I) requires that the owner or operator of the protected computer must authorize the interception of the trespasser's communications. Second, section 2511(2)(i)(II) requires that the person who intercepts the communication be lawfully engaged in an ongoing investigation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation.

Third, section 2511(2)(i)(III) requires that the person acting under color of law have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. Fourth, section 2511(2)(i)(IV) requires that investigators intercept only the communications sent or received by trespassers. Thus, this section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting users authorized to use the computer.

Finally, section 217 of the Act amends section 2510 of title 18 to create a definition of "computer trespasser." Such trespassers include any person who accesses a protected computer (as defined in section 1030 of title 18)[5] without authorization. In addition, the definition explicitly excludes any person "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator for access to all or part of the computer." 18 U.S.C. § 2510(21). For example, certain Internet service providers do not allow their customers to send bulk unsolicited e-mails (or "spam"). Customers who send spam would be in violation of the provider's terms of service, but would not qualify as trespassers – both because they are authorized users and because they have an existing contractual relationship with the provider. These provisions will sunset December 31, 2005.

* * *

**SEC. 219. SINGLE-JURISDICTION SEARCH WARRANTS FOR TERRORISM.**

Rule 41(a) of the Federal Rules of Criminal Procedure is amended by inserting after `executed' the following: `and (3) in an investigation of domestic terrorism or international terrorism (as defined in section 2331 of title 18, United States Code), by a Federal magistrate judge in any district in which activities related to the terrorism may have occurred, for a search of property or for a person within or outside the district'.

SUMMARY: Under prior law, Rule 41(a) of the Federal Rules of Criminal Procedure required that a search warrant be obtained within a district for searches within that district. The only exception was for cases in which property or a person within the district might leave the district prior to execution of the warrant. The rule created unnecessary delays and burdens for the government in the investigation of terrorist activities and networks that spanned a number of districts, since warrants must be separately obtained in each district.

Section 219 resolves that problem by providing that, in domestic or international terrorism cases, a search warrant may be issued by a magistrate judge in any district in which activities related to the terrorism have occurred for a search of property or persons located within or outside of the district.

**SEC. 220. NATIONWIDE SERVICE OF SEARCH WARRANTS FOR ELECTRONIC EVIDENCE.**

(a) IN GENERAL- Chapter 121 of title 18, United States Code, is amended--

(1) in section 2703, by striking `under the Federal Rules of Criminal Procedure' every place it appears and inserting `using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction

[5] Section 1030 defines a protected computer as any computer used in interstate or foreign commerce, as well as most computers used by financial institutions or the U.S. Government. Thus, almost any computer connected to the Internet qualifies as a "protected computer."

over the offense under investigation'; and
(2) in section 2711--
(A) in paragraph (1), by striking `and';
(B) in paragraph (2), by striking the period and inserting `; and'; and
(C) by inserting at the end the following:
`(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.'.
(b) CONFORMING AMENDMENT- Section 2703(d) of title 18, United States Code, is amended by striking `described in section 3127(2)(A)'.

SUMMARY: Section 2703(a) requires the government to use a search warrant to compel a provider to disclose unopened e-mail less than six months old. Because Rule 41 of the Federal Rules of Criminal Procedure requires that the "property" to be obtained be "within the district" of the issuing court, however, some courts have declined to issue section 2703(a) warrants for e-mail located in other districts. Unfortunately, this refusal has placed an enormous administrative burden on those districts in which major ISPs are located, such as the Eastern District of Virginia and the Northern District of California, even though these districts may have no relationship with the criminal acts under investigation. In addition, requiring investigators to obtain warrants in distant jurisdictions has slowed time-sensitive investigations.

*Amendment:* Section 220 of the Act amends section 2703(a) of title 18 (and parallel provisions elsewhere in section 2703) to allow investigators to use section 2703(a) warrants to compel records outside of the district in which the court is located, just as they use federal grand jury subpoenas and orders under section 2703(d). This change enables courts with jurisdiction over investigations to compel evidence directly, without requiring the intervention of agents, prosecutors, and judges in the districts where major ISPs are located. This provision will sunset December 31, 2005.

* * *

**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.

SUMMARY: Both the House and Senate bills included this provision that this Act does not impose any additional technical requirements on a provider of a wire or electronic communication service and that 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 expenditures incurred in providing such facilities or assistance. Not in original Administration proposal.

**SEC. 223. CIVIL LIABILITY FOR CERTAIN UNAUTHORIZED DISCLOSURES.**

(a) Section 2520 of title 18, United States Code, is amended--
(1) in subsection (a), after `entity', by inserting `, other than the United States,';
(2) by adding at the end the following:
`(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 reasons for such determination.'; and
(3) by adding a new subsection (g), as follows:
`(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 purposes of section 2520(a).'.

(b) Section 2707 of title 18, United States Code, is amended--

(1) in subsection (a), after `entity', by inserting `, other than the United States,';

(2) by striking subsection (d) and inserting the following:

`(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 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.'; and

(3) by adding a new subsection (g), as follows:

`(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.'.

(c)(1) Chapter 121 of title 18, United States Code, is amended by adding at the end the following:

`Sec. 2712. Civil actions against the United States

`(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 U.S.C. 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 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.'.

(2) The table of sections at the beginning of chapter 121 is amended to read as follows:

`2712. Civil action against the United States.'.

SUMMARY: H.R. 2975 included this provision to create civil liability for violations, including unauthorized disclosures, by law enforcement authorities of the electronic surveillance procedures set forth in title 18, United States Code (e.g., unauthorized disclosure of pen trap, wiretap, stored communications), or FISA information. Also requires administrative discipline of officials who engage in such unauthorized disclosures. Not in original Administration proposal.

**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.

SUMMARY: H.R. 3162 provides a 4-year sunset for sections 206, 201, 202, 203(b), 204, 206, 207, 209, 210, 212, 214, 215, 217, 218, 220, 223 -- at the end December 31, 2005, with the authorities "grandfathered" as to particular investigations based on offenses occurring prior to sunset. No sunset provided in original Administration proposal or S. 1510, and four-year sunset shorter than the five-year sunset in H.R. 2975.

* * *

**TITLE V--REMOVING OBSTACLES TO INVESTIGATING TERRORISM**

* * *

**SEC. 503. DNA IDENTIFICATION OF TERRORISTS AND OTHER VIOLENT OFFENDERS.**

Section 3(d)(2) of the DNA Analysis Backlog Elimination Act of 2000 (42 U.S.C. 14135a(d)(2)) is amended to read as follows:

`(2) In addition to the offenses described in paragraph (1), the following offenses shall be treated for purposes of this section as qualifying Federal offenses, as determined by the Attorney General:

`(A) Any offense listed in section 2332b(g)(5)(B) of title 18, United States Code.

`(B) Any crime of violence (as defined in section 16 of title 18, United States Code).

`(C) Any attempt or conspiracy to commit any of the above offenses.'.

SUMMARY: Under prior law, the statutory provisions governing the collection of DNA samples from convicted federal offenders (42 U.S.C. § 14135a(d)) have been restrictive and, in particular, have not included persons convicted for the crimes that are most likely to be committed by terrorists. DNA samples could not be collected even from persons federally convicted of terrorist murders in many circumstances.

Section 503 addressed that deficiency, and generally strengthened the collection of DNA samples from federal offenders, by extending sample collection to all federal offenders convicted of the types of offenses that are likely to be committed by terrorists (as set forth in 18 U.S.C. § 2332b(g)(5)(B)) or any crime of violence (as defined in 18 U.S.C. §16).

* * *

**SEC. 505. MISCELLANEOUS NATIONAL SECURITY AUTHORITIES.**

(a) TELEPHONE TOLL AND TRANSACTIONAL RECORDS- Section 2709(b) of title 18, United States Code, is amended--

(1) in the matter preceding paragraph (1), by inserting `at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director' after `Assistant Director';

(2) in paragraph (1)--

(A) by striking `in a position not lower than Deputy Assistant Director'; and

(B) by striking `made that' and all that follows and inserting the following: `made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and'; and

(3) in paragraph (2)--

(A) by striking `in a position not lower than Deputy Assistant Director'; and

(B) by striking `made that' and all that follows and inserting the following: `made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.'.

(b) FINANCIAL RECORDS- Section 1114(a)(5)(A) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)(A)) is amended--

(1) by inserting `in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director' after `designee'; and

(2) by striking `sought' and all that follows and inserting `sought for foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.'.

(c) CONSUMER REPORTS- Section 624 of the Fair Credit Reporting Act (15 U.S.C. 1681u) is amended--

(1) in subsection (a)--

(A) by inserting `in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director' after `designee' the first place it appears; and

(B) by striking `in writing that' and all that follows through the end and inserting the following: `in writing, that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.';

(2) in subsection (b)--

(A) by inserting `in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director' after `designee' the first place it appears; and

(B) by striking `in writing that' and all that follows through the end and inserting the following: `in writing that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.'; and

(3) in subsection (c)--

(A) by inserting `in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director' after `designee of the Director'; and

(B) by striking `in camera that' and all that follows through `States.' and inserting the following: `in camera that the consumer report is sought for the conduct of an authorized investigation to protect against

international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.'.

SUMMARY: Both the House and Senate bills included this provision to modify current statutory provisions on access to telephone, bank, and credit records in counterintelligence investigations to remove the "agent of a foreign power" standard. The authority may be used only for investigations to protect against international terrorism or clandestine intelligence activities, and an investigation of a United States person may not be based solely on activities protected by the First Amendment. Narrower than original Administration proposal which simply removed "agent of foreign power" requirement.

* * *

## TITLE VII--INCREASED INFORMATION SHARING FOR CRITICAL INFRASTRUCTURE PROTECTION

### SEC. 701. EXPANSION OF REGIONAL INFORMATION SHARING SYSTEM TO FACILITATE FEDERAL-STATE-LOCAL LAW ENFORCEMENT RESPONSE RELATED TO TERRORIST ATTACKS.

Section 1301 of title I of the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. 3796h) is amended--

(1) in subsection (a), by inserting `and terrorist conspiracies and activities' after `activities';

(2) in subsection (b)--

(A) in paragraph (3), by striking `and' after the semicolon;

(B) by redesignating paragraph (4) as paragraph (5); and

(C) by inserting after paragraph (3) the following:

`(4) establishing and operating secure information sharing systems to enhance the investigation and prosecution abilities of participating enforcement agencies in addressing multi-jurisdictional terrorist conspiracies and activities; and (5)'; and

(3) by inserting at the end the following:

`(d) AUTHORIZATION OF APPROPRIATION TO THE BUREAU OF JUSTICE ASSISTANCE- There are authorized to be appropriated to the Bureau of Justice Assistance to carry out this section $50,000,000 for fiscal year 2002 and $100,000,000 for fiscal year 2003.'.

SUMMARY: Both the House and Senate bills included this provision to expand the Department of Justice Regional Information Sharing Systems (RISS) Program to facilitate information sharing among Federal, State and local law enforcement agencies to investigate and prosecute terrorist conspiracies and activities and doubles its authorized funding for FY2002 and FY2003. Currently, 5,700 Federal, State and local law enforcement agencies participate in the RISS Program. Not in original Administration proposal.

## TITLE VIII--STRENGTHENING THE CRIMINAL LAWS AGAINST TERRORISM

### SEC. 801. TERRORIST ATTACKS AND OTHER ACTS OF VIOLENCE AGAINST MASS TRANSPORTATION SYSTEMS.

Chapter 97 of title 18, United States Code, is amended by adding at the end the following:

`Sec. 1993. Terrorist attacks and other acts of violence against mass transportation systems

`(a) GENERAL PROHIBITIONS- Whoever willfully--

`(1) wrecks, derails, sets fire to, or disables a mass transportation vehicle or ferry;

`(2) places or causes to be placed any biological agent or toxin for use as a weapon, destructive substance, or destructive device in, upon, or near a mass transportation vehicle or ferry, without previously obtaining the permission of the mass transportation provider, and with intent to endanger the safety of any passenger or employee of the mass transportation provider, or with a reckless disregard for the safety of human life;

`(3) sets fire to, or places any biological agent or toxin for use as a weapon, destructive substance, or destructive device in, upon, or near any garage, terminal, structure, supply, or facility used in the operation of, or in support of the operation of, a mass transportation vehicle or ferry, without previously obtaining the permission of the mass transportation provider, and knowing or having reason to know such activity would likely derail, disable, or wreck a mass transportation vehicle or ferry used, operated, or employed by the mass transportation provider;

`(4) removes appurtenances from, damages, or otherwise impairs the operation of a mass transportation signal system, including a train control system, centralized dispatching system, or rail grade crossing warning signal without authorization from the mass transportation provider;

`(5) interferes with, disables, or incapacitates any dispatcher, driver, captain, or person while they are employed in dispatching, operating, or maintaining a mass transportation vehicle or ferry, with intent to endanger the safety of any passenger or employee of the mass transportation provider, or with a reckless disregard for the safety of human life;

`(6) commits an act, including the use of a dangerous weapon, with the intent to cause death or serious bodily injury to an employee or passenger of a mass transportation provider or any other person while any of the foregoing are on the property of a mass transportation provider;

`(7) conveys or causes to be conveyed false information, knowing the information to be false, concerning an attempt or alleged attempt being made or to be made, to do any act which would be a crime prohibited by this subsection; or

`(8) attempts, threatens, or conspires to do any of the aforesaid acts,

shall be fined under this title or imprisoned not more than twenty years, or both, if such act is committed, or in the case of a threat or conspiracy such act would be committed, on, against, or affecting a mass transportation provider engaged in or affecting interstate or foreign commerce, or if in the course of committing such act, that person travels or communicates across a State line in order to commit such act, or transports materials across a State line in aid of the commission of such act.

`(b) AGGRAVATED OFFENSE- Whoever commits an offense under subsection (a) in a circumstance in which--

`(1) the mass transportation vehicle or ferry was carrying a passenger at the time of the offense; or

`(2) the offense has resulted in the death of any person,

shall be guilty of an aggravated form of the offense and shall be fined under this title or imprisoned for a term of years or for life, or both.

`(c) DEFINITIONS- In this section--

`(1) the term `biological agent' has the meaning given to that term in section 178(1) of this title;

`(2) the term `dangerous weapon' has the meaning given to that term in section 930 of this title;

`(3) the term `destructive device' has the meaning given to that term in section 921(a)(4) of this title;

`(4) the term `destructive substance' has the meaning given to that term in section 31 of this title;

`(5) the term `mass transportation' has the meaning given to that term in section 5302(a)(7) of title 49, United States Code, except that the term shall include schoolbus, charter, and sightseeing transportation;

`(6) the term `serious bodily injury' has the meaning given to that term in section 1365 of this title;

`(7) the term `State' has the meaning given to that term in section 2266 of this title; and

`(8) the term `toxin' has the meaning given to that term in section 178(2) of this title.'.

(f) CONFORMING AMENDMENT- The analysis of chapter 97 of title 18, United States Code, is amended by adding at the end:

`1993. Terrorist attacks and other acts of violence against mass transportation systems.'.

SUMMARY: Section 801 created a new offense codified at 18 U.S.C. § 1993, prohibiting various violent offenses against mass transportation systems, vehicles, facilities, or passengers. The provision prohibits disabling or wrecking a mass transportation vehicle; placing a biological agent or destructive substance or device in a mass transportation vehicle with intent to endanger safety or with reckless disregard for human life; setting fire to or placing a biological agent or destructive substance or device in a mass transportation facility knowing or having reason to know that the activity is likely to disable or wreck a mass transportation vehicle; disabling mass transportation signaling systems; interfering with personnel with intent to endanger safety or with reckless disregard for human life; use of a dangerous weapon with intent to cause death or serious bodily injury to a person on the property of a mass transportation provider; conveying false information about any such offense; and attempt and conspiracy. The provision carries a maximum sentence of 20 years imprisonment, or life imprisonment if the crime results in death.

**SEC. 802. DEFINITION OF DOMESTIC TERRORISM.**

(a) DOMESTIC TERRORISM DEFINED- Section 2331 of title 18, United States Code, is amended--

(1) in paragraph (1)(B)(iii), by striking `by assassination or kidnapping' and inserting `by mass destruction, assassination, or kidnapping';

(2) in paragraph (3), by striking `and';

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

(4) by adding at the end the following:

`(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.'.
(b) CONFORMING AMENDMENT- Section 3077(1) of title 18, United States Code, is amended to read as follows:
`(1) `act of terrorism' means an act of domestic or international terrorism as defined in section 2331;'.

SUMMARY: Section 802 added to 18 U.S.C. § 2331 a new definition of "domestic terrorism," corresponding to the existing definition of "international terrorism." The term is defined to mean activities occurring primarily within the territorial jurisdiction of the United States involving acts dangerous to human life that are a violation of the criminal laws of the United States or any state and appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by mass destruction, assassination, or kidnaping. The provision also makes a minor conforming change in the definition of "international terrorism."

The definition is used in other provisions of the Act, including the provision allowing nationwide service of search warrants in cases of international or domestic terrorism.

**SEC. 803. PROHIBITION AGAINST HARBORING TERRORISTS.**

(a) IN GENERAL- Chapter 113B of title 18, United States Code, is amended by adding after section 2338 the following new section:

`Sec. 2339. Harboring or concealing terrorists

`(a) Whoever harbors or conceals any person who he knows, or has reasonable grounds to believe, has committed, or is about to commit, an offense under section 32 (relating to destruction of aircraft or aircraft facilities), section 175 (relating to biological weapons), section 229 (relating to chemical weapons), section 831 (relating to nuclear materials), paragraph (2) or (3) of section 844(f) (relating to arson and bombing of government property risking or causing injury or death), section 1366(a) (relating to the destruction of an energy facility), section 2280 (relating to violence against maritime navigation), section 2332a (relating to weapons of mass destruction), or section 2332b (relating to acts of terrorism transcending national boundaries) of this title, section 236(a) (relating to sabotage of nuclear facilities or fuel) of the Atomic Energy Act of 1954 (42 U.S.C. 2284(a)), or section 46502 (relating to aircraft piracy) of title 49, shall be fined under this title or imprisoned not more than ten years, or both.'.

`(b) A violation of this section may be prosecuted in any Federal judicial district in which the underlying offense was committed, or in any other Federal judicial district as provided by law.'.

(b) TECHNICAL AMENDMENT- The chapter analysis for chapter 113B of title 18, United States Code, is amended by inserting after the item for section 2338 the following:

`2339. Harboring or concealing terrorists.'.

SUMMARY: Section 803 created a new offense codified at 18 U.S.C. § 2339 that prohibits harboring or concealing persons who have committed or are about to commit a variety of terrorist offenses, including destruction of aircraft or aircraft facilities, use of nuclear materials or chemical or biological weapons, use of weapons of mass destruction, arson or bombing of government property, destruction of energy facilities, sabotage of nuclear facilities, or aircraft piracy. The harboring offense of prior law prohibited only the harboring of spies (see 18 U.S.C. §792); there was no comparable terrorism provision, though the harboring of terrorists creates a risk to national security readily comparable to that posed by harboring spies.

**SEC. 804. JURISDICTION OVER CRIMES COMMITTED AT U.S. FACILITIES ABROAD.**

Section 7 of title 18, United States Code, is amended by adding at the end the following:

`(9) With respect to offenses committed by or against a national of the United States as that term is used in section 101 of the Immigration and Nationality Act--

`(A) the premises of United States diplomatic, consular, military or other United States Government missions or entities in foreign States, including the buildings, parts of buildings, and land appurtenant or ancillary thereto or used for purposes of those missions or entities, irrespective of ownership; and

`(B) residences in foreign States and the land appurtenant or ancillary thereto, irrespective of ownership, used for purposes of those missions or entities or used by United States personnel assigned to those missions or entities.

Nothing in this paragraph shall be deemed to supersede any treaty or international agreement with which this

paragraph conflicts. This paragraph does not apply with respect to an offense committed by a person described in section 3261(a) of this title.'.

SUMMARY: Section 804 explicitly extended the special maritime and territorial jurisdiction of the United States to U.S. diplomatic and consular premises and related private residences overseas for offenses committed by or against a U.S. national. When offenses are committed by or against a U.S. national abroad at such U.S. facilities, the country in which the offense occurs may have little interest in prosecuting the case. Unless the United States is able to prosecute such offenders, these crimes may go unpunished. Section 804 clarified inconsistent prior caselaw to establish that the United States may prosecute offenses committed in its missions abroad, by or against its nationals. The provision explicitly exempts offenses committed by members or employees of the U.S. armed forces and persons accompanying the armed forces, who are covered under a provision of existing law, 18 U.S.C. § 3261(a).

**SEC. 805. MATERIAL SUPPORT FOR TERRORISM.**

(a) IN GENERAL- Section 2339A of title 18, United States Code, is amended--

(1) in subsection (a)--

(A) by striking `, within the United States,';

(B) by inserting `229,' after `175,';

(C) by inserting `1993,' after `1992,';

(D) by inserting `, section 236 of the Atomic Energy Act of 1954 (42 U.S.C. 2284),' after `of this title';

(E) by inserting `or 60123(b)' after `46502'; and

(F) by inserting at the end the following: `A violation of this section may be prosecuted in any Federal judicial district in which the underlying offense was committed, or in any other Federal judicial district as provided by law.'; and

(2) in subsection (b)--

(A) by striking `or other financial securities' and inserting `or monetary instruments or financial securities'; and

(B) by inserting `expert advice or assistance,' after `training,'.

(b) TECHNICAL AMENDMENT- Section 1956(c)(7)(D) of title 18, United States Code, is amended by inserting `or 2339B' after `2339A'.

SUMMARY: 18 U.S.C. § 2339A prohibits providing material support or resources to terrorists. The prior definition of "material support or resources" was generally not broad enough to encompass expert advice and assistance – for example, advice provided by a civil engineer on destroying a building, or advice by a biochemist on making a biological agent more lethal. Section 805 amends 18 U.S.C.§ 2339A to include expert advice and assistance, making the offense applicable to experts who provide advice or assistance knowing or intending that it is to be used in preparing for or carrying out terrorism crimes. Section 805 also eliminates language in § 2339A restricting its application to material support provided within the United States, and adds to the list of underlying terrorism crimes for which provision of material support is barred. Other provisions in the section provide that material support offenses can be prosecuted in any district in which the underlying offense was committed, and make it clear that prohibited material support includes all types of monetary instruments.

**SEC. 806. ASSETS OF TERRORIST ORGANIZATIONS.**

Section 981(a)(1) of title 18, United States Code, is amended by inserting at the end the following:

`(G) All assets, foreign or domestic--

`(i) of any individual, entity, or organization engaged in planning or perpetrating any act of domestic or international terrorism (as defined in section 2331) against the United States, citizens or residents of the United States, or their property, and all assets, foreign or domestic, affording any person a source of influence over any such entity or organization;

`(ii) acquired or maintained by any person with the intent and for the purpose of supporting, planning, conducting, or concealing an act of domestic or international terrorism (as defined in section 2331) against the United States, citizens or residents of the United States, or their property; or

`(iii) derived from, involved in, or used or intended to be used to commit any act of domestic or international terrorism (as defined in section 2331) against the United States, citizens or residents of the United States, or their property.'.

SUMMARY: Prior law did not specifically provide authority for the confiscation of terrorist assets. Instead, forfeiture was authorized only in narrow circumstances for the proceeds of murder, arson, and some terrorism offenses, or for laundering the

proceeds of such offenses. However, most terrorism offenses do not yield "proceeds," and available forfeiture laws required detailed tracing that is quite difficult for accounts coming through the banks of countries used by many terrorists.

Section 806 increases the government's ability to strike at terrorist organizations' economic base by permitting the forfeiture of their property regardless of the source of the property, and regardless of whether the property has actually been used to commit a terrorism offense. This is similar in concept to the forfeiture now available under RICO. In parity with the drug forfeiture laws, the section also authorizes the forfeiture of property used or intended to be used to facilitate a terrorist act, regardless of its source.

Section 806 amends 18 U.S.C. § 981(a)(1) to include a new subparagraph (G) which makes the following property subject to civil forfeiture:

"(G) All assets, foreign or domestic—

"(i) of any individual, entity or organization engaged in planning or perpetrating any act of domestic terrorism or international terrorism (as defined in section 2331) against the United States, citizens or residents of the United States, or their property, and all assets, foreign or domestic, affording any person a source of influence over any such entity or organization;

"(ii) acquired or maintained by any person with the intent and for the purpose of supporting, planning, conducting, or concealing an act of domestic terrorism or international terrorism (as defined in section 2331) against the United States, citizens or residents of the United States, or their property; or

"(iii) derived from, involved in, or used or intended to be used to commit any act of domestic terrorism or international terrorism (as defined in section 2331) against the United States, citizens or residents of the United States, or their property.".

Prosecutors are encouraged to check with AFMLS before commencing any civil forfeiture action based on section 981(a)(1)(G) so that we may coordinate application of the new law.

**SEC. 807. TECHNICAL CLARIFICATION RELATING TO PROVISION OF MATERIAL SUPPORT TO TERRORISM.**

No provision of the Trade Sanctions Reform and Export Enhancement Act of 2000 (title IX of Public Law 106-387) shall be construed to limit or otherwise affect section 2339A or 2339B of title 18, United States Code.

SUMMARY: The Trade Sanctions Reform and Export Enhancement Act of 2000, Title IX of Public Law 106-387, creates exceptions in the nation's Trade Sanctions Programs for food and agricultural products. Section 807 makes clear that the Trade Sanctions Reform and Export Enhancement Act of 2000 does not limit 18 U.S.C. §§ 2339A or 2339B. In other words, the exceptions to trade sanctions for these items does not prevent criminal liability for the provision of these items to support terrorist activity or to foreign terrorist organizations as described in 2339A and 2339B. This is not a change from existing law, but rather serves to foreclose any possible misunderstanding or argument that the Act in some manner trumps or limits the prohibition on providing material support or resources to terrorism.

**SEC. 808. DEFINITION OF FEDERAL CRIME OF TERRORISM.**

Section 2332b of title 18, United States Code, is amended--

(1) in subsection (f), by inserting `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,' before `and the Secretary'; and

(2) in subsection (g)(5)(B), by striking clauses (i) through (iii) and inserting the following:

`(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.'.

SUMMARY: Section 808 added several offenses, including a number of aircraft violence crimes and certain computer crimes, to the list of predicate offenses in the definition of "Federal crime of terrorism" that appears in 18 U.S.C. § 2332b(g)(5). That term is defined as any of a comprehensive list of offenses likely to be committed by terrorists (set forth in § 2332b(g)(5)(B)) if calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct. The list of predicate crimes in § 2332b(g)(5)(B) is used elsewhere in the Act to define the scope of other provisions, including a longer statute of limitations (section 809), lengthened periods of supervised release (section 812), and additional crimes that are now RICO predicates (section 813).

Because of Congressional concerns about overbreadth, this section removes some crimes from prior § 2332b(g)(5)(B) (primarily offenses involving assault and less grave property crimes). To fully preserve the Attorney General's primary investigatory authority over these offenses, section 808 includes a conforming amendment to § 2332b(f) which explicitly adds these offenses to that provision.

**SEC. 809. NO STATUTE OF LIMITATION FOR CERTAIN TERRORISM OFFENSES.**

(a) IN GENERAL- Section 3286 of title 18, United States Code, is amended to read as follows:

`Sec. 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 forseeable risk of, death or serious bodily injury to another person.'.

(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.

SUMMARY: Most non-capital federal offenses are subject to a five-year statute of limitations; under prior law, many terrorism offenses were subject to an eight-year statute of limitations under 18 U.S.C. § 3286. Section 809 expands the list of offenses subject to the eight-year limitation period to include all offenses listed in § 2332b(g)(5)(B), unless otherwise subject

to a longer limitation period. In addition, section 809 provides that any offense listed in § 2332b(g)(5)(B) may be prosecuted without limitation of time if the offense resulted in, or created a foreseeable risk of, death or serious bodily injury to a person other than the defendant. This will make it possible to prosecute the perpetrators of such terrorist acts whenever they are identified and apprehended.

The section expressly provides that it is applicable to offenses committed before the date of enactment of the statute, as well as those committed thereafter. This retroactivity provision ensures that the section's limitation period reforms will apply, for example, to the prosecution of crimes committed in connection with the September 11, 2001 terrorist attacks. The constitutionality of such retroactive applications of changes in statutes of limitations is well settled. *See, e.g., United States v. Grimes*, 142 F.3d 1342, 1350-51 (11th Cir. 1998); *People v. Frazer*, 982 P.2d 180 (Cal. 1999).

**SEC. 810. ALTERNATE MAXIMUM PENALTIES FOR TERRORISM OFFENSES.**

(a) ARSON- Section 81 of title 18, United States Code, is amended in the second undesignated paragraph by striking `not more than twenty years' and inserting `for any term of years or for life'.

(b) DESTRUCTION OF AN ENERGY FACILITY- Section 1366 of title 18, United States Code, is amended--

(1) in subsection (a), by striking `ten' and inserting `20'; and

(2) by adding at the end the following:

`(d) Whoever is convicted of a violation of subsection (a) or (b) that has resulted in the death of any person shall be subject to imprisonment for any term of years or life.'.

(c) MATERIAL SUPPORT TO TERRORISTS- Section 2339A(a) of title 18, United States Code, is amended--

(1) by striking `10' and inserting `15'; and

(2) by striking the period and inserting `, and, if the death of any person results, shall be imprisoned for any term of years or for life.'.

(d) MATERIAL SUPPORT TO DESIGNATED FOREIGN TERRORIST ORGANIZATIONS- Section 2339B(a)(1) of title 18, United States Code, is amended--

(1) by striking `10' and inserting `15'; and

(2) by striking the period after `or both' and inserting `, and, if the death of any person results, shall be imprisoned for any term of years or for life.'.

(e) DESTRUCTION OF NATIONAL-DEFENSE MATERIALS- Section 2155(a) of title 18, United States Code, is amended--

(1) by striking `ten' and inserting `20'; and

(2) by striking the period at the end and inserting `, and, if death results to any person, shall be imprisoned for any term of years or for life.'.

(f) SABOTAGE OF NUCLEAR FACILITIES OR FUEL- Section 236 of the Atomic Energy Act of 1954 (42 U.S.C. 2284), is amended--

(1) by striking `ten' each place it appears and inserting `20';

(2) in subsection (a), by striking the period at the end and inserting `, and, if death results to any person, shall be imprisoned for any term of years or for life.'; and

(3) in subsection (b), by striking the period at the end and inserting `, and, if death results to any person, shall be imprisoned for any term of years or for life.'.

(g) SPECIAL AIRCRAFT JURISDICTION OF THE UNITED STATES- Section 46505(c) of title 49, United States Code, is amended--

(1) by striking `15' and inserting `20'; and

(2) by striking the period at the end and inserting `, and, if death results to any person, shall be imprisoned for any term of years or for life.'.

(h) DAMAGING OR DESTROYING AN INTERSTATE GAS OR HAZARDOUS LIQUID PIPELINE FACILITY- Section 60123(b) of title 49, United States Code, is amended--

(1) by striking `15' and inserting `20'; and

(2) by striking the period at the end and inserting `, and, if death results to any person, shall be imprisoned for any term of years or for life.'.

SUMMARY: Section 810 amended existing statutes prescribing punishment levels for crimes likely to be committed by terrorists that previously were subject to inadequate maximum penalties. This section provides for enhanced maximum penalties for arson offenses under 18 U.S.C. § 81, destruction of an energy facility under § 1366, material support to terrorists under § 2339A, material support to designated foreign terrorist organizations under § 2339B, destruction of national-defense materials under § 2155(a), sabotage of nuclear facilities or fuel under 42 U.S.C. § 2284, carrying weapons aboard aircraft

with reckless disregard for human life under 49 U.S.C. § 46505(c), and damaging or destroying an interstate gas or hazardous liquid pipeline facility under 49 U.S.C. § 60123(b).

**SEC. 811. PENALTIES FOR TERRORIST CONSPIRACIES.**

(a) ARSON- Section 81 of title 18, United States Code, is amended in the first undesignated paragraph--

(1) by striking `, or attempts to set fire to or burn'; and

(2) by inserting `or attempts or conspires to do such an act,' before `shall be imprisoned'.

(b) KILLINGS IN FEDERAL FACILITIES- Section 930(c) of title 18, United States Code, is amended--

(1) by striking `or attempts to kill';

(2) by inserting `or attempts or conspires to do such an act,' before `shall be punished'; and

(3) by striking `and 1113' and inserting `1113, and 1117'.

(c) COMMUNICATIONS LINES, STATIONS, OR SYSTEMS- Section 1362 of title 18, United States Code, is amended in the first undesignated paragraph--

(1) by striking `or attempts willfully or maliciously to injure or destroy'; and

(2) by inserting `or attempts or conspires to do such an act,' before `shall be fined'.

(d) BUILDINGS OR PROPERTY WITHIN SPECIAL MARITIME AND TERRITORIAL JURISDICTION- Section 1363 of title 18, United States Code, is amended--

(1) by striking `or attempts to destroy or injure'; and

(2) by inserting `or attempts or conspires to do such an act,' before `shall be fined' the first place it appears.

(e) WRECKING TRAINS- Section 1992 of title 18, United States Code, is amended by adding at the end the following:

`(c) A person who conspires to commit any offense defined in this section shall be subject to the same penalties (other than the penalty of death) as the penalties prescribed for the offense, the commission of which was the object of the conspiracy.'.

(f) MATERIAL SUPPORT TO TERRORISTS- Section 2339A of title 18, United States Code, is amended by inserting `or attempts or conspires to do such an act,' before `shall be fined'.

(g) TORTURE- Section 2340A of title 18, United States Code, is amended by adding at the end the following:

`(c) CONSPIRACY- A person who conspires to commit an offense under this section shall be subject to the same penalties (other than the penalty of death) as the penalties prescribed for the offense, the commission of which was the object of the conspiracy.'.

(h) SABOTAGE OF NUCLEAR FACILITIES OR FUEL- Section 236 of the Atomic Energy Act of 1954 (42 U.S.C. 2284), is amended--

(1) in subsection (a)--

(A) by striking `, or who intentionally and willfully attempts to destroy or cause physical damage to';

(B) in paragraph (4), by striking the period at the end and inserting a comma; and

(C) by inserting `or attempts or conspires to do such an act,' before `shall be fined'; and

(2) in subsection (b)--

(A) by striking `or attempts to cause'; and

(B) by inserting `or attempts or conspires to do such an act,' before `shall be fined'.

(i) INTERFERENCE WITH FLIGHT CREW MEMBERS AND ATTENDANTS- Section 46504 of title 49, United States Code, is amended by inserting `or attempts or conspires to do such an act,' before `shall be fined'.

(j) SPECIAL AIRCRAFT JURISDICTION OF THE UNITED STATES- Section 46505 of title 49, United States Code, is amended by adding at the end the following:

`(e) CONSPIRACY- If two or more persons conspire to violate subsection (b) or (c), and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be punished as provided in such subsection.'.

(k) DAMAGING OR DESTROYING AN INTERSTATE GAS OR HAZARDOUS LIQUID PIPELINE FACILITY- Section 60123(b) of title 49, United States Code, is amended--

(1) by striking `, or attempting to damage or destroy,'; and

(2) by inserting `, or attempting or conspiring to do such an act,' before `shall be fined'.

SUMMARY: While many terrorism offenses contain specific provisions punishing conspiracies with the same maximum penalties as substantive offenses, under prior law, some did not. If no specific conspiracy provisions existed, the alternative was proceeding under the general conspiracy provision (18 U.S.C. § 371), which carries a maximum penalty of five years even if the object of the conspiracy is a serious crime carrying a far higher maximum penalty. Section 811 amended several criminal statutes to provide adequate conspiracy penalties by authorizing maximum penalties equal to the completed offense.

Section 811 created enhanced conspiracy penalties for arson under 18 U.S.C. § 81, killings in federal facilities under § 930(c), injuring or destroying communications lines or systems under § 1362, injuring or destroying buildings or property within the special maritime and territorial jurisdiction of the United States under § 1363, wrecking trains under § 1992, material support to terrorists under § 2339A, torture under § 2340A, sabotage of nuclear facilities or fuel under 42 U.S.C. § 2284, interference with flight crew members and attendants under 49 U.S.C. § 46504, carrying weapons aboard aircraft under 49 U.S.C. § 46505, and damaging or destroying an interstate gas or hazardous liquid pipeline facility under 49 U.S.C. § 60123(b).

**SEC. 812. POST-RELEASE SUPERVISION OF TERRORISTS.**

Section 3583 of title 18, United States Code, is amended by adding at the end the following:

`(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.'.

SUMMARY: Prior federal law (18 U.S.C. § 3583(b)) generally capped the maximum period of post-imprisonment supervision for released felons at 3 or 5 years. Thus, for a released but unreformed terrorist, there was no means of tracking the person or imposing conditions to prevent renewed involvement in terrorist activities beyond a period of a few years. The drug laws (21 U.S.C. § 841) mandate longer supervision periods for persons convicted of certain drug trafficking crimes, and specify no upper limit on the duration of supervision, but there was nothing comparable for terrorism offenses.

Section 812 added a new subsection to 18 U.S.C. § 3583 to authorize longer supervision periods, including potentially lifetime supervision, for persons convicted of certain terrorism crimes. This permits appropriate tracking and oversight following release of offenders whose involvement with terrorism may reflect lifelong ideological commitments. The covered class of crimes is the crimes listed in 18 U.S.C. § 2332b(g)(5)(B), where the commission of the offense resulted in, or created a foreseeable risk of, death or serious injury to another person.

**SEC. 813. INCLUSION OF ACTS OF TERRORISM AS RACKETEERING ACTIVITY.**

Section 1961(1) of title 18, United States Code, is amended--

(1) by striking `or (F)' and inserting `(F)'; and

(2) by inserting before the semicolon at the end the following: `, or (G) any act that is indictable under any provision listed in section 2332b(g)(5)(B)'.

SUMMARY: Under prior law, the list of predicate federal offenses for RICO, appearing in 18 U.S.C. § 1961(1), did not include the offenses which are most likely to be committed by terrorists. Section 813 added the crimes listed in § 2332b(g)(5)(B) to the list of RICO predicates, which will make it possible to use RICO more readily in the prosecution of terrorist organizations.

**SEC. 814. DETERRENCE AND PREVENTION OF CYBERTERRORISM.**

(a) CLARIFICATION OF PROTECTION OF PROTECTED COMPUTERS- Section 1030(a)(5) of title 18, United States Code, is amended--

(1) by inserting `(i)' after `(A)';

(2) by redesignating subparagraphs (B) and (C) as clauses (ii) and (iii), respectively;

(3) by adding `and' at the end of clause (iii), as so redesignated; and

(4) by adding at the end the following:

`(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;'.

(b) PROTECTION FROM EXTORTION- Section 1030(a)(7) of title 18, United States Code, is amended by striking `, firm, association, educational institution, financial institution, government entity, or other legal entity,'.

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

(1) in paragraph (2)--

(A) in subparagraph (A) --

(i) by inserting `except as provided in subparagraph (B),' before `a fine';

(ii) by striking `(a)(5)(C)' and inserting `(a)(5)(A)(iii)'; and

(iii) by striking `and' at the end;

(B) in subparagraph (B), by inserting `or an attempt to commit an offense punishable under this subparagraph,' after `subsection (a)(2),' in the matter preceding clause (i); and

(C) in subparagraph (C), by striking `and' at the end;

(2) in paragraph (3)--

(A) by striking `, (a)(5)(A), (a)(5)(B),' both places it appears; and

(B) by striking `(a)(5)(C)' and inserting `(a)(5)(A)(iii)'; and

(3) by adding at the end the following:

`(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) DEFINITIONS- Section 1030(e) of title 18, United States Code is amended--

(1) in paragraph (2)(B), by inserting `, 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' before the semicolon;

(2) in paragraph (7), by striking `and' at the end;

(3) by striking paragraph (8) and inserting the following:

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

(4) in paragraph (9), by striking the period at the end and inserting a semicolon; and

(5) by adding at the end the following:

`(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' means 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.'.

(e) DAMAGES IN CIVIL ACTIONS- Section 1030(g) of title 18, United States Code is amended--

(1) by striking the second sentence and inserting the following: `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.'; and

(2) by adding at the end the following: `No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.'.

(f) 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.

SUMMARY: Section 814 makes a number of changes to improve 18 U.S.C. § 1030, the Computer Fraud and Abuse Act. This section increases penalties for hackers who damage protected computers (from a maximum of 10 years to a maximum of 20 years); clarifies the *mens rea* required for such offenses to make explicit that a hacker need only intend damage, not a

particular *type* of damage; adds a new offense for damaging computers used for national security or criminal justice; expands the coverage of the statute to include computers in foreign countries so long as there is an effect on U.S. interstate or foreign commerce; counts state convictions as "prior offenses" for purpose of recidivist sentencing enhancements; and allows losses to several computers from a hacker's course of conduct to be aggregated for purposes of meeting the $5,000 jurisdictional threshold.

The following discussion analyzes these and other provisions in more detail.

1. Section 1030(c) - Raising the maximum penalty for hackers that damage protected computers and eliminating mandatory minimums

*Previous law:* Under previous law, first-time offenders who violate section 1030(a)(5) could be punished by no more than five years' imprisonment, while repeat offenders could receive up to ten years. Certain offenders, however, can cause such severe damage to protected computers that this five-year maximum did not adequately take into account the seriousness of their crimes. For example, David Smith pled guilty to violating section 1030(a)(5) for releasing the "Melissa" virus that damaged thousands of computers across the Internet. Although Smith agreed, as part of his plea, that his conduct caused over $80,000,000 worth of loss (the maximum dollar figure contained in the Sentencing Guidelines), experts estimate that the real loss was as much as ten times that amount.

In addition, previous law set a mandatory sentencing guidelines minimum of six months imprisonment for any violation of section 1030(a)(5), as well as for violations of section 1030(a)(4) (accessing a protected computer with the intent to defraud).

*Amendment*: Section 814 of the Act raises the maximum penalty for violations for damaging a protected computer to ten years for first offenders, and twenty years for repeat offenders. 18 U.S.C. § 1030(c)(4). Congress chose, however, to eliminate all mandatory sentencing guidelines minimums for section 1030 violations.

2. Subsection 1030(c)(2)(C) and (e)(8) - Hackers need only intend to cause damage, not a particular consequence or degree of damage

*Previous law:* Under previous law, in order to violate subsections (a)(5)(A), an offender had to "intentionally [cause] damage without authorization." Section 1030 defined "damage" as impairment to the integrity or availability of data, a program, a system, or information that (1) caused loss of at least $5,000; (2) modified or impairs medical treatment; (3) caused physical injury; or (4) threatened public health or safety.

The question repeatedly arose, however, whether an offender must *intend* the $5,000 loss or other special harm, or whether a violation occurs if the person only intends to damage the computer, *that in fact* ends up causing the $5,000 loss or harming the individuals. It appears that Congress never intended that the language contained in the definition of "damage" would create additional elements of proof of the actor's mental state. Moreover, in most cases, it would be almost impossible to prove this additional intent.

*Amendment:* Section 814 of the Act restructures the statute to make clear that an individual need only intend to damage the computer or the information on it, and not a specific dollar amount of loss or other special harm. The amendments move these jurisdictional requirements to 1030(a)(5)(B), explicitly making them elements of the offense, and define "damage" to mean "*any* impairment to the integrity or availability of data, a program, a system or information." 18 U.S.C. § 1030(e)(8) (emphasis supplied). Under this clarified structure, in order for the government to prove a violation of 1030(a)(5), it must show that the actor caused damage to a protected computer (with one of the listed mental states), and that the actor's conduct caused either loss exceeding $5,000, impairment of medical records, harm to a person, or threat to public safety. 18 U.S.C. § 1030(a)(5)(B).

3. Section 1030(c) - Aggregating the damage caused by a hacker's entire course of conduct

*Previous law:* Previous law was unclear about whether the government could aggregate the loss resulting from damage an individual caused to different protected computers in seeking to meet the jurisdictional threshold of $5,000 in loss. For example, an individual could unlawfully access five computers on a network on ten different dates — as part of a related course of conduct — but cause only $1,000 loss to each computer during each intrusion. If previous law were interpreted not

to allow aggregation, then that person would not have committed a federal crime at all since he or she had not caused over $5,000 to any particular computer.

*Amendment:* Under the amendments in Section 814 of the Act, the government may now aggregate "loss resulting from a related course of conduct affecting one or more other protected computers" that occurs within a one year period in proving the $5,000 jurisdictional threshold for damaging a protected computer. 18 U.S.C. § 1030(a)(5)(B)(i).

4. 1030(c)(2)(C) - New offense for damaging computers used for national security and criminal justice

*Previous law*: Section 1030 previously had no special provision that would enhance punishment for hackers who damage computers used in furtherance of the administration of justice, national defense, or national security. Thus, federal investigators and prosecutors did not have jurisdiction over efforts to damage criminal justice and military computers where the attack did not cause over $5,000 loss (or meet one of the other special requirements). Yet these systems serve critical functions and merit felony prosecutions even where the damage is relatively slight. Indeed, attacks on computers used in the national defense that occur during periods of active military engagement are particularly serious — even if they do not cause extensive damage or disrupt the war-fighting capabilities of the military — because they divert time and attention away from the military's proper objectives. Similarly, disruption of court computer systems and data could seriously impair the integrity of the criminal justice system.

*Amendment:* Amendments in Section 814 of the Act create section 1030(a)(5)(B)(v) to solve this inadequacy. Under this provision, a hacker violates federal law by damaging a computer "used by or for a government entity in furtherance of the administration of justice, national defense, or national security," even if that damage does not result in provable loss over $5,000.

5. Subsection 1030(e)(2) - expanding the definition of "protected computer" to include computers in foreign countries

*Previous law:* Before the amendments in Section 814 of the Act, section 1030 of title 18 defined "protected computer" as a computer used by the federal government or a financial institution, or one "which is used in interstate or foreign commerce." 18 U.S.C. § 1030(e)(2). The definition did not explicitly include computers outside the United States.

Because of the interdependency and availability of global computer networks, hackers from within the United States are increasingly targeting systems located entirely outside of this country. The statute did not explicitly allow for prosecution of such hackers. In addition, individuals in foreign countries frequently route communications through the United States, even as they hack from one foreign country to another. In such cases, their hope may be that the lack of any U.S. victim would either prevent or discourage U.S. law enforcement agencies from assisting in any foreign investigation or prosecution.

*Amendment*: Section 814 of the Act amends the definition of "protected computer" to make clear that this term includes computers outside of the United States so long as they affect "interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B). By clarifying the fact that a domestic offense exists, the United States can now use speedier domestic procedures to join in international hacker investigations. As these crimes often involve investigators and victims in more than one country, fostering international law enforcement cooperation is essential.

In addition, the amendment creates the option, where appropriate, of prosecuting such criminals in the United States. Since the U.S. is urging other countries to ensure that they can vindicate the interests of U.S. victims for computer crimes that originate in their nations, this provision will allow the U.S. to provide reciprocal coverage.

6. Subsection 1030(e)(10) - counting state convictions as "prior offenses"

*Previous law:* Under previous law, the court at sentencing could, of course, consider the offender's prior convictions for State computer crime offenses. State convictions, however, did not trigger the recidivist sentencing provisions of section 1030, which double the maximum penalties available under the statute.

*Amendment*: Section 814 of the Act alters the definition of "conviction" so that it includes convictions for serious computer hacking crimes under State law – *i.e.*, State felonies where an element of the offense is "unauthorized access, or exceeding authorized access, to a computer." 18 U.S.C. § 1030(e)(10).

7. Subsection 1030(e)(11) -- Definition of "loss"

*Previous law:* Calculating "loss" is important where the government seeks to prove that an individual caused over $5,000 loss in order to meet the jurisdictional requirements found in 1030(a)(5)(B)(i). Yet prior to the amendments in Section 814 of the Act, section 1030 of title 18 had no definition of "loss." The only court to address the scope of the definition of loss adopted an inclusive reading of what costs the government may include. In United States v. Middleton, 231 F.3d 1207, 1210-11 (9th Cir. 2000), the court held that the definition of loss includes a wide range of harms typically suffered by the victims of computer crimes, including costs of responding to the offense, conducting a damage assessment, restoring the system and data to their condition prior to the offense, and any lost revenue or costs incurred because of interruption of service.

*Amendments*: Amendments in Section 814 codify the appropriately broad definition of loss adopted in Middleton. 18 U.S.C. § 1030(e)(11).

**SEC. 815. ADDITIONAL DEFENSE TO CIVIL ACTIONS RELATING TO PRESERVING RECORDS IN RESPONSE TO GOVERNMENT REQUESTS.**

Section 2707(e)(1) of title 18, United States Code, is amended by inserting after `or statutory authorization' the following: `(including a request of a governmental entity under section 2703(f) of this title)'.

SUMMARY: Section 815 added to an existing defense to a cause for damages for violations of the Electronic Communications Privacy Act, Chapter 121 of Title 18. Under prior law it was a defense to such a cause of action to rely in good faith on a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization. This amendment makes clear that the "statutory authorization" defense includes good-faith reliance on a government request to preserve evidence under 18 U.S.C. § 2703(f).

**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 relating 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.

SUMMARY: Section 816 requires the Attorney General to establish such regional computer forensic laboratories as he considers appropriate, and to provide support for existing computer forensic laboratories, to enable them to provide certain forensic and training capabilities. The provision also authorizes the spending of money to support those laboratories.

**SEC. 817. EXPANSION OF THE BIOLOGICAL WEAPONS STATUTE.**

Chapter 10 of title 18, United States Code, is amended--

(1) in section 175--

(A) in subsection (b)--

(i) by striking `does not include' and inserting `includes';

(ii) by inserting `other than' after `system for'; and

(iii) by inserting `bona fide research' after `protective';

(B) by redesignating subsection (b) as subsection (c); and

(C) by inserting after subsection (a) the following:

`(b) ADDITIONAL OFFENSE- Whoever knowingly possesses any biological agent, toxin, or delivery system of a type or in a quantity that, under the circumstances, is not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose, shall be fined under this title, imprisoned not more than 10 years, or both. In this subsection, the terms `biological agent' and `toxin' do not encompass any biological agent or toxin that is in its naturally occurring environment, if the biological agent or toxin has not been cultivated, collected, or otherwise extracted from its natural source.';

(2) by inserting after section 175a the following:

`SEC. 175b. POSSESSION BY RESTRICTED PERSONS.

`(a) No restricted person described in subsection (b) shall ship or transport interstate or foreign commerce, or possess in or affecting commerce, any biological agent or toxin, or receive any biological agent or toxin that has been shipped or transported in interstate or foreign commerce, if the biological agent or toxin is listed as a select agent in subsection (j) of section 72.6 of title 42, Code of Federal Regulations, pursuant to section 511(d)(l) of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104-132), and is not exempted under subsection (h) of such section 72.6, or appendix A of part 72 of the Code of Regulations.

`(b) In this section:

`(1) The term `select agent' does not include any such biological agent or toxin that is in its naturally-occurring environment, if the biological agent or toxin has not been cultivated, collected, or otherwise extracted from its natural source.

`(2) The term `restricted person' means an individual who--

`(A) is under indictment for a crime punishable by imprisonment for a term exceeding 1 year;

`(B) has been convicted in any court of a crime punishable by imprisonment for a term exceeding 1 year;

`(C) is a fugitive from justice;

`(D) is an unlawful user of any controlled substance (as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802));

`(E) is an alien illegally or unlawfully in the United States;

`(F) has been adjudicated as a mental defective or has been committed to any mental institution;

`(G) is an alien (other than an alien lawfully admitted for permanent residence) who is a national of a country as to which the Secretary of State, pursuant to section 6(j) of the Export Administration Act of 1979 (50 U.S.C. App. 2405(j)), section 620A of chapter 1 of part M of the Foreign Assistance Act of 1961 (22 U.S.C. 2371), or section 40(d) of chapter 3 of the Arms Export Control Act (22 U.S.C. 2780(d)), has made a determination (that remains in effect) that such country has repeatedly provided support for acts of international terrorism; or

`(H) has been discharged from the Armed Services of the United States under dishonorable conditions.

`(3) The term `alien' has the same meaning as in section 1010(a)(3) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(3)).

`(4) The term `lawfully admitted for permanent residence' has the same meaning as in section 101(a)(20) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(20)).

`(c) Whoever knowingly violates this section shall be fined as provided in this title, imprisoned not more than 10 years, or both, but the prohibition contained in this section shall not apply with respect to any duly authorized United States governmental activity.'; and

(3) in the chapter analysis, by inserting after the item relating to section 175a the following:

`175b. Possession by restricted persons.'.

SUMMARY: Section 817 expanded the coverage of existing restrictions on the possession and use of biological agents and toxins. Prior law prohibited the possession, development, acquisition, etc., of biological agents or toxins “for use as a weapon.” 18 U.S.C. § 175. Section 817 amended the definition of “for use as a weapon” to include all situations in which it can be proven that the defendant had any purpose other than a prophylactic, protective, bona fide research, or other peaceful purpose. This enhances the government’s ability to prosecute suspected terrorists in possession of biological agents or toxins, and conforms the scope of the criminal offense in 18 U.S.C. § 175 more closely to the related forfeiture provision in 18 U.S.C. § 176.

Moreover, the section added a subsection to 18 U.S.C. § 175 which defines an additional offense of possessing a biological agent or toxin of a type or in a quantity that, under the circumstances, is not reasonably justified by a prophylactic,

protective, bona fide research, or other peaceful purpose. Finally, this section also enacts a new statute, 18 U.S.C. § 175b, which generally makes it an offense for certain restricted persons (including felons, persons indicted for felonies, fugitives, drug users, illegal aliens, mentally impaired persons, aliens from certain terrorist states, and persons dishonorably discharged from the U.S. armed services) to possess a biological agent or toxin listed as a "select agent" by the Secretary of Health and Human Services.

* * *

## TITLE X--MISCELLANEOUS

* * *

**SEC. 1005. FIRST RESPONDERS ASSISTANCE ACT.**

(a) GRANT AUTHORIZATION- The Attorney General shall make grants described in subsections (b) and (c) to States and units of local government to improve the ability of State and local law enforcement, fire department and first responders to respond to and prevent acts of terrorism.

(b) TERRORISM PREVENTION GRANTS- Terrorism prevention grants under this subsection may be used for programs, projects, and other activities to--

(1) hire additional law enforcement personnel dedicated to intelligence gathering and analysis functions, including the formation of full-time intelligence and analysis units;

(2) purchase technology and equipment for intelligence gathering and analysis functions, including wire-tap, pen links, cameras, and computer hardware and software;

(3) purchase equipment for responding to a critical incident, including protective equipment for patrol officers such as quick masks;

(4) purchase equipment for managing a critical incident, such as communications equipment for improved interoperability among surrounding jurisdictions and mobile command posts for overall scene management; and

(5) fund technical assistance programs that emphasize coordination among neighboring law enforcement agencies for sharing resources, and resources coordination among law enforcement agencies for combining intelligence gathering and analysis functions, and the development of policy, procedures, memorandums of understanding, and other best practices.

(c) ANTITERRORISM TRAINING GRANTS- Antiterrorism training grants under this subsection may be used for programs, projects, and other activities to address--

(1) intelligence gathering and analysis techniques;

(2) community engagement and outreach;

(3) critical incident management for all forms of terrorist attack;

(4) threat assessment capabilities;

(5) conducting followup investigations; and

(6) stabilizing a community after a terrorist incident.

(d) APPLICATION-

(1) IN GENERAL- Each eligible entity that desires to receive a grant under this section shall submit an application to the Attorney General, at such time, in such manner, and accompanied by such additional information as the Attorney General may reasonably require.

(2) CONTENTS- Each application submitted pursuant to paragraph (1) shall--

(A) describe the activities for which assistance under this section is sought; and

(B) provide such additional assurances as the Attorney General determines to be essential to ensure compliance with the requirements of this section.

(e) MINIMUM AMOUNT- If all applications submitted by a State or units of local government within that State have not been funded under this section in any fiscal year, that State, if it qualifies, and the units of local government within that State, shall receive in that fiscal year not less than 0.5 percent of the total amount appropriated in that fiscal year for grants under this section.

(f) AUTHORIZATION OF APPROPRIATIONS- There are authorized to be appropriated $25,000,000 for each of the fiscal years 2003 through 2007.

SUMMARY: This provision authorizes grants to State and local authorities to respond to and prevent acts of terrorism. .Not in original Administration proposal.

* * *

**SEC. 1012. LIMITATION ON ISSUANCE OF HAZMAT LICENSES.**

(a) LIMITATION-

(1) IN GENERAL- Chapter 51 of title 49, United States Code, is amended by inserting after section 5103 the following new section:

`Sec. 5103a. Limitation on issuance of hazmat licenses

`(a) LIMITATION-

`(1) ISSUANCE OF LICENSES- A State may not issue to any individual a license to operate a motor vehicle transporting in commerce a hazardous material unless the Secretary of Transportation has first determined, upon receipt of a notification under subsection (c)(1)(B), that the individual does not pose a security risk warranting denial of the license.

`(2) RENEWALS INCLUDED- For the purposes of this section, the term `issue', with respect to a license, includes renewal of the license.

`(b) HAZARDOUS MATERIALS DESCRIBED- The limitation in subsection (a) shall apply with respect to--

`(1) any material defined as a hazardous material by the Secretary of Transportation; and

`(2) any chemical or biological material or agent determined by the Secretary of Health and Human Services or the Attorney General as being a threat to the national security of the United States.

`(c) BACKGROUND RECORDS CHECK-

`(1) IN GENERAL- Upon the request of a State regarding issuance of a license described in subsection (a)(1) to an individual, the Attorney General--

`(A) shall carry out a background records check regarding the individual; and

`(B) upon completing the background records check, shall notify the Secretary of Transportation of the completion and results of the background records check.

`(2) SCOPE- A background records check regarding an individual under this subsection shall consist of the following:

`(A) A check of the relevant criminal history data bases.

`(B) In the case of an alien, a check of the relevant data bases to determine the status of the alien under the immigration laws of the United States.

`(C) As appropriate, a check of the relevant international data bases through Interpol-U.S. National Central Bureau or other appropriate means.

`(d) REPORTING REQUIREMENT- Each State shall submit to the Secretary of Transportation, at such time and in such manner as the Secretary may prescribe, the name, address, and such other information as the Secretary may require, concerning--

`(1) each alien to whom the State issues a license described in subsection (a); and

`(2) each other individual to whom such a license is issued, as the Secretary may require.

`(e) ALIEN DEFINED- In this section, the term `alien' has the meaning given the term in section 101(a)(3) of the Immigration and Nationality Act.'.

(2) CLERICAL AMENDMENT- The table of sections at the beginning of such chapter is amended by inserting after the item relating to section 5103 the following new item:

`5103a. Limitation on issuance of hazmat licenses.'.

(b) REGULATION OF DRIVER FITNESS- Section 31305(a)(5) of title 49, United States Code, is amended--

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

(2) by inserting `and' at the end of subparagraph (B); and

(3) by adding at the end the following new subparagraph:

`(C) is licensed by a State to operate the vehicle after having first been determined under section 5103a of this title as not posing a security risk warranting denial of the license.'.

(c) AUTHORIZATION OF APPROPRIATIONS- There is authorized to be appropriated for the Department of Transportation and the Department of Justice such amounts as may be necessary to carry out section 5103a of title 49, United States Code, as added by subsection (a).

SUMMARY: This provision allows the Department of Transportation to obtain background records checks for any individual applying for a license to transport hazardous materials in interstate commerce. Not in original Administration proposal.

**SEC. 1013. EXPRESSING THE SENSE OF THE SENATE CONCERNING THE PROVISION OF FUNDING FOR BIOTERRORISM PREPAREDNESS AND RESPONSE.**

(a) FINDINGS- The Senate finds the following:

(1) Additional steps must be taken to better prepare the United States to respond to potential bioterrorism attacks.

(2) The threat of a bioterrorist attack is still remote, but is increasing for a variety of reasons, including--

(A) public pronouncements by Osama bin Laden that it is his religious duty to acquire weapons of mass destruction, including chemical and biological weapons;

(B) the callous disregard for innocent human life as demonstrated by the terrorists' attacks of September 11, 2001;

(C) the resources and motivation of known terrorists and their sponsors and supporters to use biological warfare;

(D) recent scientific and technological advances in agent delivery technology such as aerosolization that have made weaponization of certain germs much easier; and

(E) the increasing access to the technologies and expertise necessary to construct and deploy chemical and biological weapons of mass destruction.

(3) Coordination of Federal, State, and local terrorism research, preparedness, and response programs must be improved.

(4) States, local areas, and public health officials must have enhanced resources and expertise in order to respond to a potential bioterrorist attack.

(5) National, State, and local communication capacities must be enhanced to combat the spread of chemical and biological illness.

(6) Greater resources must be provided to increase the capacity of hospitals and local health care workers to respond to public health threats.

(7) Health care professionals must be better trained to recognize, diagnose, and treat illnesses arising from biochemical attacks.

(8) Additional supplies may be essential to increase the readiness of the United States to respond to a bio-attack.

(9) Improvements must be made in assuring the safety of the food supply.

(10) New vaccines and treatments are needed to assure that we have an adequate response to a biochemical attack.

(11) Government research, preparedness, and response programs need to utilize private sector expertise and resources.

(12) Now is the time to strengthen our public health system and ensure that the United States is adequately prepared to respond to potential bioterrorist attacks, natural infectious disease outbreaks, and other challenges and potential threats to the public health.

(b) SENSE OF THE SENATE- It is the sense of the Senate that the United States should make a substantial new investment this year toward the following:

(1) Improving State and local preparedness capabilities by upgrading State and local surveillance epidemiology, assisting in the development of response plans, assuring adequate staffing and training of health professionals to diagnose and care for victims of bioterrorism, extending the electronics communications networks and training personnel, and improving public health laboratories.

(2) Improving hospital response capabilities by assisting hospitals in developing plans for a bioterrorist attack and improving the surge capacity of hospitals.

(3) Upgrading the bioterrorism capabilities of the Centers for Disease Control and Prevention through improving rapid identification and health early warning systems.

(4) Improving disaster response medical systems, such as the National Disaster Medical System and the Metropolitan Medical Response System and Epidemic Intelligence Service.

(5) Targeting research to assist with the development of appropriate therapeutics and vaccines for likely bioterrorist agents and assisting with expedited drug and device review through the Food and Drug Administration.

(6) Improving the National Pharmaceutical Stockpile program by increasing the amount of necessary therapies (including smallpox vaccines and other post-exposure vaccines) and ensuring the appropriate deployment of stockpiles.

(7) Targeting activities to increase food safety at the Food and Drug Administration.

(8) Increasing international cooperation to secure dangerous biological agents, increase surveillance, and retrain biological warfare specialists.

SUMMARY: This provision expresses the sense of the Senate that the United States should make a substantial new investment this year toward improving State and local preparedness to respond to potential bioterrorism attacks. Not in original Administration proposal.

**SEC. 1014. GRANT PROGRAM FOR STATE AND LOCAL DOMESTIC PREPAREDNESS SUPPORT.**

(a) IN GENERAL- The Office for State and Local Domestic Preparedness Support of the Office of Justice Programs shall make a grant to each State, which shall be used by the State, in conjunction with units of local government, to enhance the capability of State and local jurisdictions to prepare for and respond to terrorist acts including events of terrorism involving weapons of mass destruction and biological, nuclear, radiological, incendiary, chemical, and explosive devices.

(b) USE OF GRANT AMOUNTS- Grants under this section may be used to purchase needed equipment and to provide training and technical assistance to State and local first responders.

(c) AUTHORIZATION OF APPROPRIATIONS-

(1) IN GENERAL- There is authorized to be appropriated to carry out this section such sums as necessary for each of fiscal years 2002 through 2007.

(2) LIMITATIONS- Of the amount made available to carry out this section in any fiscal year not more than 3 percent may be used by the Attorney General for salaries and administrative expenses.

(3) MINIMUM AMOUNT- Each State shall be allocated in each fiscal year under this section not less than 0.75 percent of the total amount appropriated in the fiscal year for grants pursuant to this section, except that the United States Virgin Islands, America Samoa, Guam, and the Northern Mariana Islands each shall be allocated 0.25 percent.

SUMMARY: This provision authorizes an appropriated Department of Justice program to provide grants to States to prepare for and respond to terrorist acts including but not limited to events of terrorism involving weapons of mass destruction and biological, nuclear, radiological, incendiary, chemical, and explosive devices. The authorization revises this grant program to provide: (1) additional flexibility to purchase needed equipment; (2) training and technical assistance to State and local first responders; and (3) a more equitable allocation of funds to all States. Not in original Administration proposal.

**SEC. 1015. EXPANSION AND REAUTHORIZATION OF THE CRIME IDENTIFICATION TECHNOLOGY ACT FOR ANTITERRORISM GRANTS TO STATES AND LOCALITIES.**

Section 102 of the Crime Identification Technology Act of 1998 (42 U.S.C. 14601) is amended--

(1) in subsection (b)--

(A) in paragraph (16), by striking `and' at the end;

(B) in paragraph (17), by striking the period and inserting `; and'; and

(C) by adding at the end the following:

`(18) notwithstanding subsection (c), antiterrorism purposes as they relate to any other uses under this section or for other antiterrorism programs.'; and

(2) in subsection (e)(1), by striking `this section' and all that follows and inserting `this section $250,000,000 for each of fiscal years 2002 through 2007.'.

SUMMARY: This provision adds an additional antiterrorism purpose for grants under the Crime Identification Technology Act, and authorizes grants under that Act through fiscal year 2007. Not in original Administration proposal.

* * *

END