CONFIDENTIAL—NOT FOR DISTRIBUTION
Draft—January 9, 2003

DOMESTIC SECURITY ENHANCEMENT ACT OF 2003

SECTION-BY-SECTION ANALYSIS

Title I: Enhancing National Security Authorities

Subtitle A: Foreign Intelligence Surveillance Act Amendments

Section 101: Individual Terrorists as Foreign Powers.

Under 50 U.S.C. § 1801(a)(4), the definition of "foreign power" includes groups that engage in international terrorism, but does not reach unaffiliated individuals who do so. As a result, investigations of "lone wolf" terrorists or "sleeper cells" may not be authorized under FISA. Such investigations therefore must proceed under the stricter standards and shorter time periods set forth in Title III, potentially resulting in unnecessary and dangerous delays and greater administrative burden. This provision would expand FISA's definition of "foreign power" to include *all* persons, regardless of whether they are affiliated with an international terrorist group, who engage in international terrorism.

Section 102: Clandestine Intelligence Activities by Agent of a Foreign Power.

FISA currently defines "agent of a foreign power" to include a person who knowingly engages in clandestine intelligence gathering activities on behalf of a foreign power—but only if those activities "involve or may involve a violation of" federal criminal law. Requiring the additional showing that the intelligence gathering violates the laws of the United States is both unnecessary and counterproductive, as such activities threaten the national security regardless of whether they are illegal. This provision would expand the definitions contained in 50 U.S.C. § 1801(b)(2)(A) & (B). Any person who engages in clandestine intelligence gathering activities for a foreign power would qualify as an "agent of a foreign power," regardless of whether those activities are federal crimes.

Section 103: Strengthening Wartime Authorities Under FISA.

Under 50 U.S.C. §§ 1811, 1829 & 1844, the Attorney General may authorize, without the prior approval of the FISA Court, electronic surveillance, physical searches, or the use of pen registers for a period of 15 days following a congressional declaration of war. This wartime exception is unnecessarily narrow; it may be invoked only when Congress formally has declared war, a rare event in the nation's history and something that has not occurred in more than sixty years. This provision would expand FISA's wartime exception by allowing the wartime exception

to be invoked after Congress authorizes the use of military force, or after the United States has suffered an attack creating an national emergency.

Section 104: Strengthening FISA's Presidential Authorization Exception.

50 U.S.C. § 1802 allows the Attorney General to authorize electronic surveillance for up to a year, without the FISA Court's prior approval, in two narrow circumstances: (1) if the surveillance is are directed solely at communications between foreign powers; or (2) if the surveillance is directed solely at the acquisition of technical intelligence, other than spoken communications, from property under the exclusive control of a foreign power. In addition, the Attorney General must certify that there is no substantial likelihood that such surveillance will acquire the communications of U.S. persons. (In essence, § 1802 authorizes the surveillance of communications between foreign governments, and between a foreign government and its embassy.) Section 1802 is of limited use, however, because it explicitly prohibits efforts to acquire spoken communications. (No such limitation exists in the parallel exception for physical searches, 50 U.S.C. § 1822(a), under which agents presumably could infiltrate a foreign power's property for the purpose of overhearing conversations.) This provision would enhance the presidential authorization exception by eliminating the requirement that electronic surveillance cannot be directed at the spoken communications of foreign powers.

Section 105: Law Enforcement Use of FISA Information.

50 U.S.C. § 1806(b) currently prohibits the disclosure of information "for law enforcement purposes" unless the disclosure includes a statement that the information cannot be used in a criminal proceeding without the Attorney General's advance authorization. This provision would amend § 1806(b) to give federal investigators and prosecutors greater flexibility to use FISA-obtained information. Specifically, it would eliminate the requirement that the Attorney General personally approve the use of such information in the criminal context, and would substitute a requirement that such use be approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or an Assistant Attorney General designated by the Attorney General.

Section 106: Defense of Reliance on Authorization.

50 U.S.C. §§ 1809(b) and 1827(b) create a defense for agents who engage in unauthorized surveillance or searches, or who disclose information without authorization, if they were relying on an order issued by the FISA Court. However, there does not appear to be a statutory defense for agents who engage in surveillance or searches pursuant to FISA authorities under which no prior court approval is required—e.g., pursuant to FISA's wartime exception (50 U.S.C. §§ 1811, 1829 & 1844), or FISA's presidential authorization exception (50 U.S.C. §§ 1802 & 1822(a)). This provision would clarify that the "good faith reliance" defense is available, not just when

agents are acting pursuant to a FISA Court order, but also when they are acting pursuant to a lawful authorization from the President or the Attorney General.

Section 107: Pen Registers in FISA Investigations.

50 U.S.C. § 1842(a)(1) makes FISA pen registers available in investigations of non-U.S. persons to "obtain foreign intelligence information." But for U.S. persons, the standard is much higher: in cases involving U.S. persons, pen registers are only available "to protect against international terrorism or clandestine intelligence activities." Perversely, this appears to be *stricter* than the standard for pen registers under Title III, which requires only that it be shown that the information "is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a)(1). This provision would amend § 1842(a)(1) by eliminating the stricter standard for U.S. persons. Specifically, FISA pen registers would be available in investigations of both U.S. persons and non-U.S. persons whenever they could be used "to obtain foreign intelligence information."

Section 108: Appointed Counsel in Appeals to FISA Court of Review.

Under FISA, proceedings before the FISA Court and the Court of Review are conducted ex parte. As a result, when the Court of Review meets to consider an appeal by the United States, there is no party to defend the judgment of the court below. The FISA Court of Review thus is obliged to interpret sensitive and complicated statutes without the benefit of the adversary process. This provision would amend FISA to permit the FISA Court of Review, in its discretion, to appoint a lawyer, with appropriate security credentials, to defend the judgment of the FISA Court, when the United States appeals a ruling to the FISA Court of Review. It would also provide for the compensation of a lawyer so appointed by the FISA Court of Review.

Sec. 109: Enforcement of Foreign Intelligence Surveillance Court Orders.

The Foreign Intelligence Surveillance Act does not specify the means for enforcement of orders issued by the Foreign Intelligence Surveillance Court. Thus, for example, if a person refuses to comply with an order of the court to cooperate in the installation of a pen register or trap and trace device under 50 U.S.C. § 1842(d), or an order to produce records under 50 U.S.C. § 1861, existing law provides no clearly defined recourse to secure compliance with the court's order. This section remedies this omission by providing that the Foreign Intelligence Surveillance Court has the same authority as a United States district court to enforce its orders, including the authority to impose contempt sanctions in case of disobedience.

Sec. 110: Technical Correction Related to the USA PATRIOT Act.

Section 204 of the USA PATRIOT Act clarified that intelligence exceptions from the limitations on interception and disclosure of wire, oral, and electronic communications continue to apply, notwithstanding section 216 of the Act. Section 224 sunsetted several provisions of the Act on December 31, 2005. Although section 216 was not included in the sunset provision, section 204's clarifying language was sunsetted. If not corrected, this anomaly will result in the loss of valuable and necessary intelligence exemptions to the pen register and trap and trace provisions after December 31, 2005. This provision would eliminate this anomaly and treat the clarifying language of section 204 the same as section 216.

Sec. 111. International Terrorist Organizations as Foreign Powers.

Groups engaged in international terrorism are included under the definition of "foreign power" in FISA. See 50 U.S.C. § 1801(a)(4). However, for certain purposes— including the duration of surveillance orders and the definition of what constitutes a "United States person"— they are effectively excluded from the concept of foreign powers, and accorded the more protected treatment that FISA provides to other entities. This section amends FISA so that international terrorist organizations are consistently treated as foreign powers for these purposes.

More specifically, there are basically two sets within the FISA definition of "foreign power" under 50 U.S.C. § 1801(a): (i) A paragraph (1)-(3) set, which includes foreign governments, foreign factions, and entities that foreign governments openly acknowledge they direct and control. (ii) A paragraph (4)-(6) set, which includes groups engaged in international terrorism or preparations therefor, foreign-based political organizations not substantially composed of U.S. persons, and entities directed and controlled by foreign governments.

50 U.S.C. §§ 1805(e) and 1824(d) define the authorization periods for electronic surveillance and physical searches under FISA. The basic authorization and extension periods are 90 days, but longer for surveillance and searches relating to certain foreign powers. Specifically, the authorization and extension periods for foreign powers in the paragraph (1)-(3) set— foreign governments, foreign factions, and entities for which foreign governments openly acknowledge direction and control— are up to a year. In contrast, for foreign powers in the paragraph (4)-(6) set— international terrorist organizations, foreign-base political organizations not substantially composed of U.S. persons, and entities directed and controlled by foreign governments— the initial authorization period is no more than 90 days. The extension period for foreign powers in the paragraph (4)-(6) set is also no more than 90 days, unless certain restrictions and special finding requirements are satisfied. (Specifically, the extension period may be up to a year for an order relating to a foreign-based political organization not substantially composed of U.S. persons or an order relating to an entity directed and controlled by a foreign government, and up to a year for an order relating to an international terrorist organization that is not a U.S. person, if the judge finds probable cause to believe that no communication or property of any individual U.S. person will be acquired.)

Another context in which different types of "foreign powers" are treated differently is the FISA definition of "United States person." United States persons have a more protected status under FISA for certain purposes, such as dissemination of information. The existing definition of "United States person" in 50 U.S.C. § 1801(i) categorically excludes a corporation or association which is a foreign power— but only if it falls in the paragraph (1)- (3) set.

The effect of the foregoing provisions is that, even if probable cause is established that a group is an international terrorist organization, it may be subject only to brief periods of surveillance absent renewal, and it may be accorded the protected status of a United States person. The amendments in this section will facilitate the investigation of threats to the national security posed by such groups by reassigning them to the less protected status now accorded to foreign powers in the paragraph (1)- (3) set. Thus, the normal authorization and extension periods for surveillance of international terrorist organizations would be up to a year, and corporations and associations which are international terrorist organizations would not be treated as United States persons under FISA.

Subtitle B: Enhancement of Law Enforcement Investigative Tools

Section 121: Definition of Terrorist Activities.

This section adds a definition of "terrorist activities" to the definitional section for the chapter of the criminal code governing electronic surveillance (chapter 119). The definition encompasses criminal acts of domestic and international terrorism as defined in 18 U.S.C. § 2331, together with related preparatory, material support, and criminal activities. The same definition of terrorist activities would also apply through cross-referencing provisions, see 18 U.S.C. § 2711(1) and 3127(1) (as amended), in the chapters of the criminal code that govern accessing stored communications and the use of pen registers and trap and trace devices (chapters 121 and 206).

The surveillance chapters of the criminal code contain many provisions which state that the authorized surveillance activities may be carried out as part of "criminal investigations." Section 121 also adds a provision to 18 U.S.C. § 2510 which specifies that "criminal investigations" include all investigations of criminal terrorist activities, to make it clear that the full range of authorized surveillance techniques are available in investigations of "terrorist activities" under the new definition.

Section 122: Inclusion of Terrorist Activities as Surveillance Predicates.

This section adds terrorist activities, as defined under the amendment of section 121, and four specific offenses that are likely to be committed by terrorists (the offenses defined by 18 U.S.C. §§ 37, 930(c), 956, and 1993), as explicit predicates for electronic surveillance and monitoring. It further adds an explicit reference to terrorist activities to the provision authorizing electronic

surveillance without a court order in emergency situations—18 U.S.C. § 2518(7)—and makes conforming changes in the corresponding provision (18 U.S.C. § 3125) for using pen registers and trap and trace devices without a court order in emergency situations.

The final subsection of this section modifies the definition of "court of competent jurisdiction" in 18 U.S.C. § 3127(2), to correct an unintended effect of amendments in sections 216(c)(1) and 220 of the USA PATRIOT Act. The purpose of the amendments was to authorize courts having jurisdiction over an offense to issue orders for pen registers and trap and trace devices, and search warrants for the disclosure of e-mails, which could be executed outside of their districts. However, the language utilized inadvertently created a lack of clarity concerning the continued validity of the pre-existing authority of the courts to issue such orders and warrants for execution within their own districts (regardless of whether they have "jurisdiction over the offense").

This threatens to be a serious practical problem when information gathering in the United States is needed in response to requests by foreign law enforcement agencies to assist in foreign terrorism (or other criminal investigations) and to fulfill the United States' obligations under mutual legal assistance treaties, and in the context of investigations relating to crimes committed on U.S. military bases abroad, because in those cases the U.S. courts generally do not have jurisdiction over the offense. This section corrects the problem in relation to pen register and trap and trace orders through definitional language that explicitly includes both a court with jurisdiction over the offense or activities being investigated, and a court in the district in which the order will be executed. A parallel correction for the problem relating to search warrants for e-mails appears in section 125(b) of this bill.

Section 123: Extension of Authorized Periods Relating to Surveillance and Searches in Investigations of Terrorist Activities.

In *Katz v. United States*, 389 U.S. 347 (1967), the Supreme Court held for the first time that government wiretapping was subject to the Fourth Amendment. In response, Congress enacted Title III of the 1968 Omnibus Crime Control and Safe Streets Act, 28 U.S.C. §§ 2510-2522, which governs electronic surveillance for all federal criminal offenses. Congress also subsequently enacted the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2701-2712, which addresses government access to stored communications, and established statutory standards and procedures for the use of pen registers and trap and trace devices, 18 U.S.C. §§ 3121-3127. Further, because *Katz* and progeny specifically stated that the Court did not hold that the same Fourth Amendment restrictions applied with respect to the activities of foreign powers and their agents, in 1978 Congress enacted the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1862, which establishes standards applicable to surveillance of foreign powers and agents of foreign powers—including electronic surveillance, physical searches, and use of pen registers and trap and trace devices—in relation to the investigation of such matters as international terrorism and espionage.

Congress has not provided separate statutory standards governing investigations of wholly domestic threats to the national security, particularly domestic terrorism. Thus, such investigations are subject to the time limits set forth in Title III. However, the Supreme Court in *United States v. United States District Court* ("*Keith*"), 407 U.S. 297 (1972), explicitly recognized that domestic security investigations would require different standards than those set forth in Title III:

> "We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.' The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime."

Id. at 322. Because domestic security investigations were subject to Title III, despite these considerations, the Court invited Congress to legislate new and different standards for such investigations:

> "Given [the] potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."

Id.

In *Keith*, the court noted that, with respect to surveillance in domestic security cases, "the time and reporting requirements need not be so strict as those in § 2518." *Id.* at 323. This section accepts the Court's invitation and extends, in investigations of terrorist activities, a number of statutory time limits or periods relating to electronic surveillance or monitoring and searches. The specific changes are:

(1) Amend 18 U.S.C. § 2518(5) to extend the normal duration of electronic surveillance orders in investigations of terrorist activities from 30 days to 90 days.

(2) Amend 18 U.S.C. § 2518(6), which provides that an electronic surveillance order may require periodic progress reports to the judge who issued the order "at such intervals as

the judge may require." As amended, the provision would not allow reports to be required at shorter intervals than 30 days in investigations of terrorist activities.

(3) Amend 18 U.S.C. § 2705, which permits delaying notification concerning the accessing of a person's stored electronic communications where specified "adverse results" would result from the notification. As amended, the provision would include endangerment of the national security as a specified adverse result that permits delaying notification.

(4) Amend 18 U.S.C. § 3123 to extend the normal authorization periods for pen registers and trap and trace devices in investigations of terrorist activities from 60 days to 120 days.

Section 124: Multi-function Devices

Electronic manufacturers increasingly are producing devices that are capable of performing multiple functions—e.g., cell phones that also can send e-mail like a Blackberry, and that include a calendar like a Palm Pilot. Multiple functions are also illustrated by ordinary home computers, which may, for example, be used to send and receive e-mail messages, to engage in oral communications through an Internet phone service, to store sent and received messages, and to store other information. Current law does not make it clear that the authorization (e.g., under an electronic surveillance order) to monitor one of a device's functions also entails the authority to monitor other functions.

This section accordingly amends 18 U.S.C. § 2518(4) to make it clear that authorization of electronic surveillance with respect to a device, unless otherwise specified, may be relied on to intercept and access communications through any of the device's functions. The section also effectively allows a search warrant for other information retrievable from the device (whether or not related to the intercepted communications) to be combined with the electronic surveillance order, and makes conforming changes in the chapters relating to accessing stored communications and pen registers and trap and trace devices.

The section further incorporates a correction for an unintended consequence of amendments in section 220 of the USA PATRIOT Act. As discussed in relation to section 122 of the bill above, amendments designed to authorize courts having jurisdiction over an offense to issue search warrants for the disclosure of e-mails outside of their districts have inadvertently clouded the pre-existing authority of the courts to issue such orders and warrants for execution within their own districts. This section corrects the problem by amending the pertinent language in 18 U.S.C. § 2703(b)(1)(A) and (c)(1)(A) to refer to a court in a district in which a provider of electronic communications service is located, as well as a court having jurisdiction over the offense or activities under investigation.

Section 125: Nationwide Search Warrants in Terrorism Investigations.

Federal Rule of Criminal Procedure 41(a)(3) currently authorizes judges in one district to issue search warrants that are valid in another district, if the crime being investigated is "domestic terrorism or international terrorism" as defined in 18 U.S.C. § 2331. But § 2331 sets forth an extremely narrow definition of terrorism, as it is limited to "violent acts or acts dangerous to human life." Thus section 2331 arguably does not include investigations into terrorist financing, or other crimes that terrorists are likely to commit. As a result, a federal judge sitting in New York would be able to issue a search warrant that is valid in California in an investigation of a plot to bomb a building, but arguably could not issue the same warrant if the investigation concerned the raising of money to support terrorist operations.

This provision would expand the types of terrorism crimes for which judges may issue search warrants that are valid nationwide. Specifically, it would authorize nationwide search warrants in investigations of the offenses listed in 18 U.S.C. § 2332b(g)(5)(B), including computer crimes, attacks on communications infrastructure, and providing material support to terrorists or terrorist organizations.

Section 126: Equal Access to Consumer Credit Reports.

In recent years, it has become increasingly apparent that law enforcement investigators need access to suspected terrorists' banking information to determine their connections to terrorist organizations, including financial ties. The current version of 15 U.S.C. § 1681b(a)(1) allows investigators to obtain a suspect's credit report—the first step in locating his banking records—only in response to a court order or a federal grand jury subpoena. As a result, law enforcement cannot obtain a suspect's banking information without issuing multiple time-consuming subpoenas. In some cases, it can take a series of three subpoenas—first to the credit reporting agency, then to the suspect's creditors, then to the suspect's banks—and a period of nine to 12 weeks to learn where a suspected terrorist keeps his accounts. Perversely, the law makes it far easier for private entities to obtain an individual's credit reports; under 15 U.S.C. § 1681b(a)(3)(F), a private entity can obtain—usually within minutes—a credit report on anyone in the United States so long as it has a "legitimate business need" for the information.

This provision would enable the government to obtain credit reports on virtually the same terms that private entities may. Specifically, it would amend § 1681b(a)(1) to allow law enforcement officers to obtain credit reports upon their certification that they will use the information only in connection with their duties to enforce federal law. This certification parallels the existing requirement that a private entity must have a "legitimate business need" before obtaining a credit report. In addition, to avoid alerting terrorists that they are under investigation, this provision would prohibit (absent court approval) disclosing to a consumer the fact that law enforcement has sought his credit report.

Section 127: Autopsy Authority.

Autopsies of the victims of terrorist attacks and other deadly crimes, as well as other persons, can be an effective way of obtaining information about the perpetrators. In addition to revealing the cause of death, autopsies sometimes enable law enforcement to retrieve forensic evidence (such as bomb fragments) from the deceased's body. The primary need for federal autopsy authority arises in the case of offenses, including acts of terrorism, outside the United States. At present, however, except in cases involving military personnel, the United States has no statutory authority to conduct autopsies. When a non-military United States national dies abroad as a result of a possible offense against the United States, the victim's body typically must be transported back to the United States before an autopsy can be performed; this may significantly delay both the return of the loved one's remains to family members, as well as cause significant delays in the criminal investigation.

This provision would create federal authority, in the Attorney General, to conduct autopsies when necessary or appropriate in the conduct of federal criminal investigations. This authority is not limited and may be delegated to other officers. This proposal is not intended to result in the hiring of medical examiners by federal law enforcement agencies. Rather, the autopsies will be performed by local coroners, private forensics investigators, or the Armed Forces Medical Examiner and his staff.

Section 128: Administrative Subpoenas in Terrorism Investigations.

The Department of Justice currently has the authority to issue administrative subpoenas in investigations of a wide variety of federal offenses, including health-care fraud*see* 18 U.S.C. § 3486(a)(1)(A), immigration violations,*see* 8 U.S.C. § 1225(a), and false claims against the United States, *see* 31 U.S.C. § 3733. But administrative subpoenas are not available in investigations of terrorism, even though the consequences of a terrorist attack are far more dire than committing simple fraud against the United States government. As a result, law-enforcement personnel are required to seek grand jury subpoenas before individuals who may have information relevant to a terrorism investigation can be compelled to testify or provide documents.

This provision would extend the existing administrative-subpoena authorities into investigations involving domestic or international terrorism. It also would prohibit a subpoena recipient from disclosing to any other person (except to a lawyer in order to obtain legal advice) the fact that he has received a subpoena. This proposal would not give the Justice Department a unilateral, unreviewable authority to compel production of documents relevant to a terrorism investigation. If recipients refuse to comply with subpoenas, the Justice Department would have to ask a court to enforce them. And subpoena recipients would retain the ability, as they do in other contexts, to ask a court to quash the subpoena. *See, e.g.*, *In re Administrative Subpoena, John Doe, D.P.M.*, 253 F.3d 256 (6th Cir. 2001).

Sec. 129: Strengthening Access to and Use of Information in National Security Investigations.

This section is primarily concerned with correcting problems and weaknesses in provisions authorizing the use of "national security letters." In substance, national security letters are administrative subpoenas that may be issued by FBI officials—or in some instances, other authorized government officials—to obtain specified types of records or information for use in national security investigations. The existing national security letter provisions include the following:

(1) 18 U.S.C. § 2709—Providing FBI access, in connection with investigations of international terrorism or espionage, to certain electronic communication transactional records maintained by communication service providers.

(2) Section 625(a)-(b) of the Fair Credit Reporting Act (15 U.S.C. § 1681u(a)-(b))—Providing FBI access, in connection with investigations of international terrorism or espionage, to certain consumer information maintained by consumer reporting agencies.

(3) Section 626 of the Fair Credit Reporting Act (15 U.S.C. § 1681v)—Providing access to consumer reports and other consumer information maintained by consumer reporting agencies, where needed by government agencies authorized to investigate or carry out intelligence or analysis activities related to international terrorism.

(4) Section 1114(a)(5) of the Right to Financial Privacy Act (12 U.S.C. § 3414(a)(5))—Providing FBI access, in connection with investigations of international terrorism or espionage, to financial records maintained by financial institutions.

(5) Section 802(a) of the National Security Act of 1947 (50 U.S.C. § 436(a))—Providing access by authorized investigative agencies to financial records and information, consumer reports, and travel records in relation to a person having access to classified information, based on indications that the person has disclosed or may disclose classified information to a foreign power.

Problems under these provisions include the following: (1) The statutes in which the national security letter provisions appear generally prohibit persons from disclosing that they have received these requests for information, to safeguard the integrity of the terrorism and espionage investigations in which national security letters are used. However, they specify no penalty for persons who make such unlawful disclosures. (2) While these statutes create a legal obligation for the recipient to provide the requested information, they do not specify any procedures for judicial enforcement in case the recipient refuses to comply with the request. (3) The scope of the national security letter provisions on the terrorism side is generally limited to international

terrorism; however, the distinction between international and domestic terrorism is increasingly elusive in contemporary circumstances. (4) These provisions are restrictive regarding the sharing of information among federal agencies with relevant responsibilities. This is in conflict with current needs and with the broad principles favoring the sharing of intelligence among federal agencies under the USA PATRIOT Act.

Subsection (a) of this section provides appropriate penalties for violations of the non-disclosure provisions of the national security letter provisions. Currently, 18 U.S.C. § 1510(b) makes it an offense for an officer of a financial institution to notify other persons about a grand jury subpoena or an administrative subpoena issued by the Department of Justice for records of the financial institution. The offense is punishable by up to a year of imprisonment, or up to five years of imprisonment if the disclosure was made with the intent to obstruct a judicial proceeding. Similarly, 18 U.S.C. § 1510(d) makes it an offense, punishable by up to five years of imprisonment, for an insurance company employee to notify other persons about a grand jury subpoena for records with intent to obstruct a judicial proceeding.

Subsection (a) of this section adds a parallel offense (proposed 18 U.S.C. § 1510(e)) covering violations of the non-disclosure requirements of the national security letter provisions described above. As with current 18 U.S.C. § 1510(b), the offense would be a misdemeanor punishable by up to a year of imprisonment, but would be punishable by up to five years of imprisonment if the unlawful disclosure was committed with the intent to obstruct the terrorism or espionage investigation. In addition to providing appropriate penalties for unlawful disclosure of national security letter requests, the same penalties would apply to: (i) violation of the non-disclosure requirement under 50 U.S.C. § 1861(d) for orders of the Foreign Intelligence Surveillance Court requiring the production of records, documents, and other tangible things in connection with investigations to obtain foreign intelligence information about non-United States persons or to protect against international terrorism or espionage, and (ii) violation of the non-disclosure provision of proposed 18 U.S.C. § 2332f(d) in section 129 of this bill, relating to administrative subpoenas in terrorism investigations.

The national security letter provisions make compliance with the request for information mandatory. See 12 U.S.C. § 3414(a)(5)(A); 15 U.S.C. §§ 1681u(a)-(b), 1681v(a); 18 U.S.C. § 2709(a); 50 U.S.C. § 436(c). However, they make no provision for judicial enforcement in case this legal obligation is not met. Subsection (b) of this section authorizes the Attorney General to seek judicial enforcement in such cases. This is similar, for example, to the existing judicial enforcement provision in 18 U.S.C. § 3486(c) for administrative subpoenas under that section.

Subsection (c) of this section amends the national security letter provisions relating to electronic communication transactional records, consumer credit information, and financial institution records, so that they apply in investigations of all types of terrorist activities. The specific amendments involve substituting, for current references in these provisions to

investigations relating to "international terrorism," references to investigations relating to "terrorist activities." The latter notion is defined in proposed 18 U.S.C. § 2510(20) in section 121 of this bill so as to include domestic, as well as international, terrorism. The limitation to international terrorism in existing law is an impediment to the effective use of national security letters because it may not be apparent in the early stages of a terrorism investigation—or even after it has continued for some time—whether domestic or international terrorism is involved. The Oklahoma City bombing and the anthrax letter incidents illustrate this point. Moreover, in the current circumstances, domestic terrorists who attempt to ally with or are inspired to emulate international terrorists are an increasing concern. The dangers posed to the national security by such persons may be comparable to those posed by international terrorists, and national security letters should likewise be an available tool in the investigation of their criminal activities.

Subsection (d) of this section deletes or modifies language in the national security letter provisions which unduly limits information sharing among federal agencies. For example, 18 U.S.C. § 2709 is the national security letter provision for electronic communication transactional records. Subsection (d) of § 2709 states that the FBI may disseminate information and records obtained pursuant to that section only as provided in guidelines approved by the Attorney General "for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency." The reference to guidelines that relate to "foreign intelligence collection and foreign counterintelligence investigations" is inconsistent with the amendment proposed in subsection (c) of this section to extend the scope of 18 U.S.C. § 2709 to include investigations of domestic terrorism, as well as international terrorism. The restrictive language regarding information sharing with other federal agencies is in conflict with the principles favoring broad sharing of intelligence among federal agencies under section 203 of the USA PATRIOT Act (Pub. L. 107-56).

Subsection (c) of this section accordingly deletes the restrictive language quoted above in 18 U.S.C. § 2709(d), so that it states simply that the FBI may disseminate information and records obtained under § 2709 only as provided in guidelines approved by the Attorney General. Subsection (c) also makes similar changes in the other national security letter provisions. The general effect of the amendments is to remove existing impediments to the sharing of information obtained by means of national security letters in terrorism and espionage investigations with other federal agencies having relevant responsibilities.

Title II: Protecting National Security Information

Section 201: Prohibition of Disclosure of Terrorism Investigation Detainee Information.

In certain instances, the release of information about persons detained in connection with terrorism investigations could have a substantial adverse impact on the United States' security interests, as well as the detainee's privacy. *Cf. North Jersey Media Group, Inc. v. Ashcroft*, 308 F.3d 198, 217-19 (3d Cir. 2002). Publicizing the fact that a particular alien has been detained could alert his coconspirators about the extent of the federal investigation and the imminence of their own detention, thus provoking them to flee to avoid detention and prosecution or to accelerate their terrorist plans before they can be disrupted.

Although existing Freedom of Information Act (FOIA) exemptions 7(A), 7(C), and 7(F) (5 U.S.C. § 552(b)(7)) permit the government to protect information relating to detainees, defending this interpretation through litigation requires extensive Department of Justice resources, which would be better spent detecting and incapacitate terrorists. This provision thus establishes a specific authority under Exemption 3 of the FOIA to clarify what is already implicit in various FOIA exemptions: the government need not disclose information about individuals detained in investigations of terrorism until disclosure occurs routinely upon the initiation of criminal charges.

Section 202: Distribution of "Worst Case Scenario" Information.

Section 112(r) of the Clean Air Act, 42 U.S.C. § 7412(r), requires private companies that use potentially dangerous chemicals to submit to the Environmental Protection Agency a "worst case scenario" report detailing what would be the impact on the surrounding community of release of the specified chemicals. Such reports are a roadmap for terrorists, who could use the information to plan attacks on the facilities.

This provision would revise section 112(r)(7)(H) of the Clean Air Act to better manage access to information contained in "worst case scenario" reports. This revised section would continue to allow such information to be shared with federal and state officials who are responsible for preventing or responding to accidental or criminal releases. However, the revised section will require that public access be limited to "read-only" methods, and only to those persons who live or work in the geographical area likely to be affected by a worst-case release from a facility.

Section 203: Information Relating to Capitol Buildings.

The Congressional Accountability Act of 1995, 2 U.S.C. § 1301 et seq., establishes the Office of Compliance, a congressional office that has the power to enforce OSHA standards with respect to the working conditions of legislative branch employees. OSHA often assists the Office in its work, *see* 2 U.S.C. §§ 1382(e) & 1385(b), and therefore the agency sometimes obtains security-sensitive information (e.g., the layout of government buildings, and the location of air circulation equipment and ventilation ducts). Terrorists may be able to obtain this information from OSHA via a FOIA request. To ensure that congressional officials can provide necessary information with

the assurance that it will not be publicly released, this provision makes clear that such information is exempt from disclosure under FOIA Exemption 3.

Section 204: Ex Parte Authorizations Under Classified Information Procedures Act.

Under the current version of the Classified Information Procedures Act,18 U.S.C. App. 3 §§ 1-16, courts have discretion over whether to approve the government's request for a CIPA authorization—which enables the submission of sensitive evidence ex parte and in camera. See 18 U.S.C. App. 3 § 4 ("The court *may* permit the United States to make a request for such authorization [for a protective order] in the form of a written statement to be inspected by the court alone." (emphasis added)). As a result, the government is forced to divert valuable resources to litigating this question. And even worse, a request for confidentiality itself can be a security breach: the government risks disclosing sensitive national-security information simply by explaining in open court why the information should be redacted. *See, e.g., United States v. Rezaq*, 899 F. Supp. 697, 707 (D.D.C. 1995) (government's CIPA pleadings must be served "on the defendant and then litigated in an adversarial hearing").

This provision would amend CIPA to provide that courts *shall* allow the United States to make a request for a CIPA authorization ex parte and in camera. This amendment would not affect the showing that the United States is required to make in order to obtain a protective order, but by replacing "may" with "shall," the United States will be able to obtain the court's guidance in every case in which classified information may potentially be discoverable, without risking disclosure of the very secrets that it seeks to protect. *See United States v. Klimavicius-Viloria*, 144 F.3d 1249, 1261 (9th Cir. 1998) (upholding the use under CIPA of ex parte, in camera hearings and written submissions by the government when the court is required to make discovery determinations).

Section 205: Exclusion of United States Security Requirements from Gross Income of Protected Officials.

Under current tax law, certain federal officials—those whose movements are restricted, or who are required to use specific facilities, for their physical protection in the interest of the United States' national security—may be taxed on the value of these protective "services." *See* 26 C.F.R. 1.132-5(m) (describing the circumstances under which police protection and related transportation expenses may be deemed to be working condition fringe benefits). Due to the recent terrorist threats, an increasing and variable number of government officials—including Cabinet and subcabinet officers, congressional leaders, and Justices of the Supreme Court—have begun to receive protective services, and now find themselves taxed on the value of these services.

Accordingly, this provision would add a provision to the Internal Revenue Code to clarify that required security measures jointly determined by the Secretary of the Treasury, the Attorney General, and the Director of Central Intelligence, are excludable from the gross income of the protected officials. This provision is limited to provisions from appropriate funds to be consistent with restrictions on the receipt of private funds for public purposes, and to ensure that the exclusion is limited to the public security purpose.

Section 206: Grand Jury Information in Terrorism Cases.

This section amends Rule 6(e)(2)(B) of the Federal Rules of Criminal Procedure to make witnesses and persons to whom subpoenas are directed subject to grand jury secrecy rules in cases where serious adverse consequences may otherwise result, including danger to the national security or to the life or physical safety of an individual, flight from prosecution, destruction of or tampering with evidence, intimidation of a potential witness, or other serious jeopardy to an investigation. The provision would permit witnesses and recipients of grand jury subpoenas to consult with counsel regarding the subpoena and any testimony, but would impose the same secrecy obligations on counsel.

Title III: Enhancing Investigations of Terrorist Plots

Subtitle A: Terrorism Identification Database

Section 301: Short Title.

This provision indicates that Title III, Subtitle B may be referred to as the "Terrorist Identification Database Act of 2003."

Section 302: Collection and Use of Identification Information from Suspected Terrorists and Other Sources.

Current law permits the FBI to establish an index to collect DNA identification records of persons *convicted* of certain crimes, and DNA samples recovered from crime scenes and unidentified human remains. 42 U.S.C. § 14132. However, the law does not directly address the FBI's authority to collect and use DNA samples of terrorists or those *suspected* of terrorism. It would be extremely beneficial to clarify how DNA samples from suspects, such as samples taken from unlawful combatants at Guantanamo Bay, can be used as necessary for counterterrorism and law-enforcement purposes. Section 302 would allow the Attorney General or Secretary of Defense to collect, analyze, and maintain DNA samples and other identification information from "suspected terrorists"—i.e., (1) persons suspected of engaging in terrorism as defined in 18 U.S.C. § 2331(1) & (5), or committing an offense described in 18 U.S.C. § 2332b(g)(5)(B), or persons conspiring or attempting to do so; (2) enemy combatants or other battlefield detainees;

(3) persons suspected of being members of a terrorist organization; and (4) certain classes of aliens including those engaged in activity that endangers national security.

Section 303: Establishment of Database to Facilitate Investigation and Prevention of Terrorist Activities.

This provision would allow the Attorney General to establish databases of DNA records pertaining to the terrorists or suspected terrorists from whom DNA samples or other identification information have been collected. All federal agencies, including the Department of Defense and probation offices, would be required to give the Attorney General, for inclusion in the databases, any DNA records, fingerprints, or other identification information that can be collected under this Subtitle. This provision also allows the Attorney General to use the information to detect, investigate, prosecute, prevent, or respond to terrorist activities, or other unlawful activities by suspected terrorists. In addition, the Attorney General would be able to share the information with other federal, state, local, or foreign agencies for the same purposes.

Section 304: Definitions.

This section would establish definitions for the terms "DNA sample" and "DNA analysis." It also would define "suspected terrorist," which describes the class of individuals from whom the Attorney General may acquire DNA samples and other identification information, and whose information may be included in DNA databases.

Section 305: Existing Authorities.

This provision would establish that the new authorities created by this Subtitle are in addition to any authorities that may exist under any other source of law. It also would provide that this Subtitle shall not construed to preclude the receipt, collection, analysis, maintenance, or dissemination of evidence or information pursuant to any other source of law.

Section 306: Conditions of Release.

This provision would amend several portions of the United States Code to clarify that terrorists or suspected terrorists who are under any form of federal supervision or conditional release, including parole, are subject to this Subtitle's provisions. These individuals would be in the physical custody of the United States but for an act of governmental discretion. This section would require such individuals to cooperate in the collection of a DNA sample as a condition of supervision or conditional release.

Subtitle B: Facilitating Information Sharing and Cooperation

Section 311: State and Local Information Sharing.

Section 203 and other provisions of the USA PATRIOT Act broadened authority to share information among federal agencies that may be relevant to the detection and prevention of terrorism, and to obtain otherwise confidential information for use in terrorism investigations. That Act, however, did not adequately address the need for enhanced information sharing authority in relation to state and local officials and foreign governments, who are the critical partners of the United States in investigating terrorist crimes and preventing future terrorist attacks. This section of the bill would provide further authority for sharing of consumer credit information, visa-related information, and educational records information with state and local law enforcement, thereby enacting the remainder of the information sharing proposals that have been proposed legislatively and endorsed by the Administration and the Department of Justice. *See* Letter of Assistant Attorney General Daniel J. Bryant to Honorable Patrick J. Leahy concerning S. 1615 (April 30, 2002).

Section 312: Appropriate Remedies with Respect to Law Enforcement Surveillance Activities.

During the 1970s and 1980s, some law enforcement agencies—e.g., the New York City Police Department—entered consent decrees that limit such agencies from gathering information about organizations and individuals that may be engaged in terrorist activities and other criminal wrongdoing. *See, e.g., Handschu v. Special Servs. Div.*, 605 F. Supp. 1384 (S.D.N.Y. 1985), *aff'd*, 787 F.2d 828 (2d Cir. 1986). As a result, they lack the ability to use the full range of investigative techniques that are lawful under the Constitution, and that are available to the FBI. (For example, the Attorney General's investigative guidelines authorize agents, subject to certain restrictions, to attend public places and events "on the same terms and conditions as members of the public generally.") The consent decrees also handicap officers in their efforts to share information with other law enforcement agencies, including federal law enforcement agencies such as the FBI. These problems threaten to frustrate the operations of the federal-state-local Joint Terrorism Task Forces, and could prevent effective cooperation at all levels of government in antiterrorism efforts. As the United States Court of Appeals for the Seventh Circuit explained (before September 11) in discussing one consent decree, as a result of such a decree "the public safety is insecure and the prerogatives of local government scorned. To continue federal judicial micromanagement of local investigations of domestic and international terrorist activities . . . is to undermine the federal system and to trifle with the public safety." *Alliance to End Repression v. City of Chicago*, 237 F.3d 799, 802 (7th Cir. 2001).

This proposal would discontinue most consent decrees that could impede terrorism investigations conducted by federal, state or local law enforcement agencies. It would immediately terminate most decrees that were enacted before September 11, 2001 (including New York City's). All surviving decrees would have to be necessary to correct a current and ongoing

violation of a Federal right, extend no further than necessary to correct the violation of the Federal right, and be narrowly drawn and the least intrusive means to correct the violation. This provision is modeled on the Prison Litigation Reform Act, 18 U.S.C. § 3626, which terminated many prison-related consent decrees and which repeatedly has been upheld by the courts. Section 312 does not apply to consent decrees or injunctions remedying discrimination based on race, color, religion, sex, or national origin, and therefore would not affect decrees or injunctions involving allegations of racial profiling.

Section 313: Disclosure of Information.

This provision provides protection against civil liability for businesses and their personnel who voluntarily provide information to federal law enforcement agencies to assist in the investigation and prevention of terrorist activities. The purpose of the provision is to encourage voluntary cooperation and assistance in counterterrorism efforts by private entities and individuals.

Subtitle C: Facilitating International Terrorism Investigations

Section 321: Authority to Seek Search Warrants and Orders to Assist Foreign States.

28 U.S.C. § 1782 does not clearly authorize the United States to obtain search warrants in response to requests from foreign governments; it only clearly applies to subpoenas. Nor is it clear that federal law enforcement can obtain orders under the pen register/trap and trace statute at foreign governments' requests. As a result, the United States can seek search warrants only if we have entered into a treaty with the foreign government that contains a provision authorizing us to do so (and, naturally, only if the foreign government has set forth facts sufficient to establish probable cause). The same is true of pen/trap orders. The United States therefore may find itself in a situation where it cannot assist a foreign government in one of its criminal investigations, which is hardly an effective way of encouraging foreign allies to assist our own counterterrorism investigations.

This provision would modify federal law to clarify that the United States may seek search warrants, pen/trap orders, and ECPA orders, in response to the requests of foreign governments. Doing so will enhance our ability to assist foreign law enforcement investigations, as well as promote better cooperation from foreign allies when we seek evidence from within their borders.

Section 322: Extradition Without Treaties and for Offenses Not Covered by an Existing Treaty.

Many of the United States' older extradition treaties contain "lists" or "schedules" of extraditable offenses that reflect only those serious crimes in existence at the time the treaties

were negotiated. (For example, our treaty with Egypt dates from 1874, and our treaty with Great Britain which includes Pakistan dates from the 1930s.) As a result, these older treaties often fail to include more modern offenses, such as money laundering, computer crimes, and certain crimes against children. While some old treaties are supplemented by newer multilateral terrorism treaties, extradition is possible under these newer treaties only if the other country is also a party to the multinational treaty, leaving gaps in coverage. Additionally, absent a few narrow exceptions, U.S. law permits the extradition of offenders to a foreign nation only when there is a treaty or convention in force with that country or a statute conferring such authority upon the executive branch. *See Valentine v. United States*, 299 U.S. 5, 8 (1936). At present, there are close to seventy countries in the world with which the U.S. has no extradition treaty at all. This means that the U.S. can become a "safe haven" for some foreign criminals, and that we cannot take advantage of some countries' willingness to surrender fugitives to us in the absence of an extradition treaty these nations usually require at least the possibility of reciprocity.

This provision would amend current extradition law to: (1) authorize the U.S. to extradite offenders to treaty partners for modern crimes that may not be included in our older list treaties with those countries; and (2) provide for on a case-by-case basis and with the approval of the Attorney General and the Secretary of State extradition from the United States for serious crimes even in the absence of an extradition treaty.

Title IV: Enhancing Prosecution and Prevention of Terrorist Crimes

Subtitle A: Increased Penalties and Protections Against Terrorist Acts

Section 401: Terrorism Hoaxes.

In the wake of the anthrax attacks in the fall of 2001, a number of individuals chose to perpetrate terrorism hoaxes (e.g., sending unidentified white powder in a letter with the intent that the recipient believe it to be anthrax). Such hoaxes divert law-enforcement and emergency-services resources, and thus impede our ability to respond to actual terrorist events. Current federal law does not adequately address the problem of hoaxes relating to various weapons of mass destruction. At present, the primary way to prosecute terrorism hoaxes is to use "threat" statutes—e.g., 18 U.S.C. § 2332a, which criminalizes certain threats to use a weapon of mass destruction, and 18 U.S.C. § 876, which criminalizes the use of the mails to threaten injury to a person. But some terrorism hoaxes are simply false reports that cannot easily be characterized as outright threats.

This section would amend federal law to create a new prohibition on terrorism hoaxes. In particular, it would (1) make it unlawful to knowingly convey false or misleading information, where the information reasonably may be believed, and concerns criminal activity relating to

weapons of mass destruction; (2) require criminal defendants to reimburse any person, including the United States, State and local first responders who incur expenses incident to an emergency or investigative response to the terrorism hoax; and (3) authorize a civil action for such expenses.

Section 402: Providing Material Support to Terrorism.

18 U.S.C. § 2339A's prohibition on providing material support to terrorists is unnecessarily narrow; it currently does not reach all situations where material support or resources are provided to facilitate the commission of "international terrorism." Rather, § 2339A only encompasses those acts of international terrorism which are prohibited by some other federal statute. Because, unlike the existing underlying offenses in § 2339A(a), "international terrorism" per se is not an offense under Title 18, it is prudent to establish unassailable constitutional bases for prohibiting such support. The first basis is if the material support is in or affects interstate or foreign commerce. The second basis is the regulation and control over the activities of U.S. nationals and U.S. legal entities who are outside the United States. Such control is based on, among others, the United States' constitutional foreign affairs power. In addition, this section amends the definition of "international terrorism" to make it clear that it covers acts which by their nature appear to be intended for the stated purposes. Hence, there would be no requirement to show that the defendants actually had such an intent. (There is a conforming amendment to the definition of "domestic terrorism" to maintain the existing parallel between the two definitions.)

Second, one court of appeals recently has questioned whether the current prohibition in 18 U.S.C. § 2339B on providing "training" or "personnel" to terrorist organizations designated under section 219 of the Immigration and Nationality Act are unconstitutionally vague. *See Humanitarian Law Project v. Reno*, 205 F.3d 1130 (9th Cir. 2000), *cert. denied*, 121 S. Ct. 1226 (2001). *But see United States v. Lindh*, ___ F. Supp. 2d ___ (E.D. Va. 2002) (rejecting the holding of *Humanitarian Law Project*). Subsection (b) would amend the pertinent statutes to remove any possible doubts about the scope of the prohibition. In particular, "training" would now be defined as "instruction or teaching designed to impart a specific skill." And criminal liability for "personnel" would apply to "knowingly provid[ing], attempt[ing] to provide, or conspir[ing] to provide a terrorist organization with one or more individuals (including himself) to work in concert with it or under its direction or control."

Section 403: Weapons of Mass Destruction.

At present, the federal weapons of mass destruction statute, 18 U.S.C. § 2332a, contains only one of the several constitutional bases for asserting federal jurisdiction over a terrorist attack involving weapons of mass destruction in certain circumstances: if the attack is against a person or property and "affect[s] interstate commerce." *Id.* § 2332a(a)(2). This provision would amend the statute to specifically cover property and persons in three other circumstances where federal jurisdiction constitutionally can be asserted: (1) if the mail or any facility of interstate or foreign

commerce is used in furtherance of the offense; (2) if the attacked property is used in interstate or foreign commerce, or in an activity that affects interstate or foreign commerce; or (3) if any perpetrator travels in or causes another to travel in interstate or foreign commerce in furtherance of the offense.

Second, with respect to attacks on government buildings, the WMD statute only applies to attacks on property owned by the United States. It currently does not directly criminalize attacks on foreign governments' property in the United States. This section therefore amends the statute, in new Subsection 2332a(a)(4), to provide for jurisdiction where the property against which the weapon of mass destruction is directed is property within the United States that is owned, leased, or used by a foreign government. (The term "foreign government" is defined in 18 U.S.C. § 11.)

Third, the current version of the WMD statute does not prohibit the use of chemical weapons; in fact, it expressly states that it does not apply to attacks carried out with "a chemical weapon as that term is defined in section 229F." 18 U.S.C. § 2332a(a), (b). This restriction was added in the implementing legislation for the Chemical Weapons Convention on October 22, 1998. Removing "chemical weapons" from the ambit of the WMD statute has proven improvident, as it has created needless factual confusion in situations where the WMD contains explosive materials but no toxic chemicals, and where it contains toxic chemicals in addition to the explosive material. Since most chemical weapons will always contain some explosive material in order to cause the dispersal of the toxic chemical, it makes little sense to arbitrarily limit the scope of the use of WMD statute since the damage resulting from its use can be caused by either the explosive material, or the toxic chemicals, or a combination of both. Restoring "chemical weapons" to the scope of the WMD statute eliminates a defendant's ability to make technical arguments that the prosecutor has charged under the wrong statute.

In addition to making the foregoing changes in the WMD statute, this section includes a technical amendment to 18 U.S.C. 175b (relating to biological agents and toxins), to correct a cross-reference to a related regulation which has been modified.

Section 404: Use of Encryption to Conceal Criminal Activity.

In recent years, terrorists and other criminals have begun to use encryption technology to conceal their communications when planning and conducting criminal activity. Title 18 of the United States Code currently contains no prohibition on the use of encrypted communications to plan or facilitate crimes. This proposal would amend federal law to provide that any person who, during the commission of or the attempt to commit a federal felony, knowingly and willfully uses encryption technology to conceal any incriminating communication or information relating to that felony, be imprisoned for an additional period of not fewer than 5 years. These additional penalties are warranted to deter the use of encryption technology to conceal criminal activity. In addition, it does not address the issue of whether software companies and internet service

providers should give law enforcement access to "keys" for the purposes of decoding intercepted communications.

Sec. 405. Presumption for Pretrial Detention in Cases Involving Terrorism

Defendants in federal cases who are accused of certain crimes are presumptively denied pretrial release. 18 U.S.C. § 3142(e). Specifically, for these crimes, there is a rebuttable presumption that "no condition or combination of conditions will reasonably assure the appearance of the person as required and the safety of the community." The list of crimes currently includes drug offenses carrying maximum prison terms of 10 years or more, but it does not include most terrorism offenses. Thus, persons accused of many drug offenses are presumptively to be detained before trial, but no comparable presumption exists for persons accused of most terrorist crimes.

This section would amend 18 U.S.C. § 3142(e) to presumptively deny release to persons charged with crimes listed in 18 U.S.C. § 2332b(g)(5)(B), which contains a standard list of offenses that are likely to be committed by terrorists. This presumption is warranted because of the unparalleled magnitude of the danger to the United States and its people posed by acts of terrorism, and because terrorism is typically engaged in by groups – many with international connections – that are often in a position to help their members flee or go into hiding.

In addition to adding terrorism offenses to those creating a presumption in favor of detention, this section makes conforming changes in a provision describing offenses for which pretrial detention may be considered (§ 3142(f)(1)) and in a provision identifying factors to be considered by the judicial officer in determining whether the defendant's appearance and public safety can reasonably be assured through release conditions (§ 3142(g)(1)).

Section 406: "Mass Transportation Vehicle" Technical Correction.

Richard Colvin Reid has been charged with attempting to blow up American Airlines Flight 63 with bombs concealed in his shoes, while over the Atlantic Ocean en route from Paris to Miami. The plane was immediately diverted to Boston. A federal grand jury sitting in the District of Massachusetts promptly indicted Reid on a variety of federal charges, including 18 U.S.C. § 1993, which prohibits wrecking a "mass transportation vehicle." (Section 1993 authorizes an aggravated penalty of up to life imprisonment when a passenger was on the mass transportation vehicle, whereas an ordinary charge under 18 U.S.C. § 32(b) permits only a 20-year prison term where no death resulted.)

The phrase "mass transportation" in section 1993 is defined by a cross-reference to 49 U.S.C. § 5302(a)(7) (the term also includes schoolbus, charter, and sightseeing transportation, 18 U.S.C. § 1993(c)(5)). In contrast to the phrase "mass transportation," the word "vehicle" has no

explicit definition in section 1993, nor is it defined in section 5302. Reid argued that an airplane is not a "vehicle" as that term is used in section 1993, and the district court dismissed that count of the indictment. *See United States v. Reid*, 206 F. Supp. 2d 132 (D. Mass. 2002) (citing *McBoyle v. United States*, 283 U.S. 25 (1931) (holding that an "aircraft" is not a "vehicle" under 1 U.S.C. § 4)). This proposal specifically provides a definition of "vehicle" for the purpose of 18 U.S.C. § 1993. This definition is broad, including any apparatus that may be used as a vehicle. This provision also would make technical amendments to the relevant chapter and section names.

Section 407: Acts of Terrorism Transcending National Boundaries.

18 U.S.C. § 2332b covers killings and other serious violent crimes against persons in the United States, where "conduct transcending national boundaries" is involved. Among other grounds, federal jurisdiction exists if "any facility of interstate or foreign commerce is used in furtherance of the offense," or if the offense affects interstate or foreign commerce. However, the statute's jurisdictional predicates are narrower than the limits contained in the Constitution. For example, the predicates do not include travel in interstate or foreign commerce in furtherance of the offense. This proposal would expand the bases for federal jurisdiction under § 2332b, including as a jurisdictional predicate travel in interstate or foreign commerce in furtherance of the offense.

The current version of § 2332b is deficient for the additional reason that it defines "facility of interstate or foreign commerce" to have the same meaning given that term in 18 U.S.C. § 1958(b)(2). But § 1958(b)(2) only defines "facility of *interstate* commerce" (to include "means of transportation and communication"), and makes no mention of *foreign* commerce. As a result, § 2332b is ambiguous on whether the same stipulation—that "means of transportation and communication" constitute a "facility of . . . commerce"—applies with respect to facilities of foreign commerce. This section therefore would correct 18 U.S.C. § 1958(b)(2) so that it refers to "facility of interstate or foreign commerce" rather than simply "facility of interstate commerce."

Section 408: Postrelease Supervision of Terrorists.

Section 812 of the USA PATRIOT Act added 18 U.S.C. § 3583(j), which authorizes up to lifetime postrelease supervision for the perpetrators of terrorist offenses. In contrast, the maximum supervision period for the most serious crimes under the general rule of 18 U.S.C. § 3583(b) is five years, and for most offenses it is three years or less. The reform adopted in the USA PATRIOT Act reflects the continuing danger to the United States and its people that convicted terrorists may pose even after completion of a term of imprisonment, and legislative recognition that involvement by offenders in terrorism may be the result of persistent (or lifelong) ideological commitments that will not simply disappear within a few years of release.

This section of the bill makes conforming amendments needed to ensure the effectiveness of the USA PATRIOT Act reform. In part, it makes conforming amendments in provisions affecting re-imprisonment on revocation of supervised release based on violations of release conditions. Currently, 18 U.S.C. § 3583(e)(3) limits imprisonment following revocation to five years in case of a class A felony, three years in case of a class B felony, two years in case of a class C or D felony, and one year otherwise. The amendments in this section do not change these maximum periods of reimprisonment, but they amend § 3583(e)(3) to make it clear that they are limitations on reimprisonment based on a particular revocation, rather than limits on aggregate reimprisonment for an offender who persistently violates release conditions and is subject to multiple revocations on that basis.

The bill also makes a complementary change in 18 U.S.C. § 3583(h). Section 3583(h) currently provides that the court may impose a term of supervised release to follow reimprisonment based on revocation of release—but not if the maximum reimprisonment term allowed by § 3583(e)(3) was imposed. Thus, the court is barred from imposing the maximum reimprisonment term—even if the maximum term is fully warranted by the nature of the offender's violation of release conditions and resulting danger to the public—if the court wants to preserve the option of providing further supervision for the offender once the term of reimprisonment is over. Since this limitation works against the effective supervision of released terrorists and protection of the public, the bill proposes that it be eliminated.

In addition, this section provides that the sentence for a terrorist offense within the scope of 18 U.S.C. § 3583(j) must include a term of supervised release of at least 10 years. By way of comparison, provisions of the drug laws that authorize extended postrelease supervision periods for certain drug offenses mandate that the sentence impose supervision terms of at least 10 years, eight years, six years, five years, four years, three years, two years, or one year for various offenses and offenders. *See* 21 U.S.C. § 841. The corresponding proposal for terrorists in this bill reflects the judgment that persons convicted of terrorist crimes generally pose a sufficient public safety concern that they should uniformly be subject to observation for a substantial period of time following release. This does not curtail the court's normal authority to revisit the period of supervision imposed in the sentence at any time after one year of release, and to shorten or terminate supervision if appropriate. *See* 18 U.S.C. § 3583(e)(1). It does, however, reflect a judgment that the period of monitoring and oversight for offenders convicted of terrorist crimes should at least be 10 years following release, unless the court affirmatively determines thereafter that further supervision is unwarranted.

This section broadens the class of offenses subject to extended supervision periods under 18 U.S.C. § 3583(j) by deleting a limitation to offenses which result in, or create a foreseeable risk of, death or serious injury. With this amendment, the provision includes all offenses in the standard list of crimes likely to be committed by terrorists and supporters of terrorism (see 18 U.S.C. § 2332b(g)(5)(B)). The existing limitation could complicate or prevent the imposition of

appropriate supervision periods on persons convicted of non-violent terrorist offenses—such as a cyberterrorism attack on the United States that results in tens of billions of dollars of economic damage—and on persons who provide the essential financial or other material support for the apparatus of terrorism, but do not directly engage themselves in violent terrorist acts. The continuing danger posed to the national security by such persons may be no less than that posed by the direct perpetrators of terrorist violence, and the courts should be afforded the same degree of discretion in prescribing postrelease supervision in their cases.

Section 409: Suspension, Revocation, and Denial of Certificates for Civil Aviation or National Security Reasons.

This section provides procedures for the suspension, revocation, and denial of pilot certificates in relation to persons who pose a threat to civil aviation or national security. There is an immediate practical need for clarification and confirmation of the authority of the Under Secretary of Transportation for Security and the Federal Aviation Administration (FAA) in this area because there are several pending challenges to FAA revocations by persons whose certificates were revoked following notification that they "were known to pose, or suspected of posing, a risk of air piracy or terrorism or a threat to airline or passenger safety" (49 U.S.C. § 114(h)(2)).

Section 410: No Statute of Limitations for Terrorism Crimes.

This section broadens the class of offenses that may be prosecuted without limitation of time under 18 U.S.C. § 3286(b) by deleting a limitation to offenses which result in, or create a foreseeable risk of, death or serious injury. With this amendment, the provision includes all offenses in the standard list of crimes likely to be committed by terrorists and supporters of terrorism (see 18 U.S.C. § 2332b(g)(5)(B)). The existing limitation could complicate or prevent the prosecution of persons convicted of non-violent terrorist offenses—such as a cyberterrorism attack on the United States that results in tens of billions of dollars of economic damage—and of persons who provide the essential financial or other material support for the apparatus of terrorism, but do not directly engage themselves in violent terrorist acts. The continuing danger posed to the national security by such persons may be no less than that posed by the direct perpetrators of terrorist violence, and they should not be entitled to permanent immunity from prosecution merely because they have succeeded in avoiding identification and apprehension for some period of time.

Section 411: Penalties for terrorist murders.

Existing law does not consistently provide adequate maximum penalties for fatal acts of terrorism. For example, in a case in which a terrorist caused massive loss of life by sabotaging a national defense installation in violation of 18 U.S.C. § 2155, sabotaging a nuclear facility in

violation of 42 U.S.C. §.2284, or destroying an energy facility in violation of 18 U.S.C. § 1366, there would be no possibility of imposing the death penalty under the statutes defining these offenses because they contain no death penalty authorizations.

In contrast, dozens of other federal violent crime provisions authorize up to life imprisonment or the death penalty in cases where victims are killed. There are also cross-cutting provisions which authorize these sanctions for specified classes of offenses whenever death results, such as 18 U.S.C. § 2245, which provides that a person who, in the course of a sexual abuse offense, "engages in conduct that results in the death of a person, shall be punished by death or imprisoned for any term of years or for life."

This section similarly authorizes uniformly up to life imprisonment or the death penalty for conduct resulting in death that occurs in the course of the offenses likely to be committed by terrorists that are listed in 18 U.S.C. § 2232b(g)(5)(B) or in the course of terrorist activities as defined in 18 U.S.C. § 2510 under the amendment in section 121 of this bill.

This section also adds the new provision covering terrorist offenses resulting in death (proposed 18 U.S.C. § 2339D) to the list of offenses in 18 U.S.C. § 3592(c)(1) whose commission permits the jury to consider imposition of the death penalty. This will make the option of capital punishment available more consistently in cases involving fatal terrorist crimes. The imposition of capital punishment in such cases will continue to be subject to the requirement under 18 U.S.C. § 3591 that the offender have a high degree of culpability with respect to the death of the victim or victims, and to the requirement that the jury conclude that the death penalty is warranted under the standards and procedures of 18 U.S.C. § 3593.

Subtitle B: Incapacitating Terrorism Financing

Section 421: Increased Penalties for Terrorism Financing.

At present, the maximum civil penalty for violations of the International Emergency Economic Powers Act, 50 U.S.C. § 1701 et seq., is only $10,000 per violation, *see* 50 U.S.C. § 1705. This is a relatively mild maximum fine; the civil penalty for violations of the Clean Water Act, for example, is fully $25,000 for each day the violation persists. *See* 33 U.S.C. § 1319(d). IEEPA's modest civil penalty may not adequately deter individuals who are considering engaging in economic transactions that finance terrorist organizations, or otherwise trading with prohibited persons. And given the severity of terrorist threats, and the consequences of a successful terrorist attack, the United States should be able to punish those who finance terrorism at least as severely as it can punish polluters. This proposal therefore would amend IEEPA to increase the maximum civil penalty amount from $10,000 per violation to $50,000 per violation.

Section 422: Money Laundering Through Hawalas

Under federal law, a financial transaction constitutes a money laundering offense only if the funds involved in the transaction represent the proceeds of some criminal offense. *See* 18 U.S.C. § 1956(a)(1) ("represents the proceeds of some form of unlawful activity"); 18 U.S.C. § 1957(f)(2) ("property constituting, or derived from, proceeds obtained from a criminal offense"). There is some uncertainty, however, as to whether the "proceeds element" is satisfied as to all aspects of a money laundering scheme when two or more transactions are conducted in parallel. For example, consider the following transaction: A sends drug proceeds to B, who deposits the money in Bank Account 1. Simultaneously or subsequently, B takes an equal amount of money from Bank Account 2 and sends it to A, or to a person designated by A. The first transaction from A to B clearly satisfies the proceeds element of the money laundering statute, but there is some question as to whether second transaction—the one that involves only funds withdrawn from Bank Account 2—does so. The question has become increasingly important because such parallel transactions are the technique used to launder money through hawalas and the Black Market Peso Exchange.

Several courts have addressed related issues, holding that both parts of the parallel or later transaction (sometimes called a "dependent" transaction because it would not have occurred but for the first transaction) involve criminal proceeds for purposes of the money laundering statute. *See United States v. Covey*, 232 F.3d 641 (8th Cir. 2000) (where defendant receives cash from drug dealer, and gives drug dealer checks drawn on own funds in return, transfer of checks is a money laundering offense involving SUA proceeds);*United States v. Mankarious*, 151 F.3d 694 (7th Cir. 1998) (if check constituting SUA proceeds is deposited in bank account, and second check is written on that account, second check constitutes proceeds, even if first check has not yet cleared); *United States v. Farrington*, 2000 WL 1751996 (D.V.I. 2000) (if check constituting SUA proceeds is deposited into bank account, and second check is drawn on same account on same day, second check is SUA proceeds, even though first check has not yet cleared). This proposal is intended to remove all uncertainty on this point by providing that all constitute parts of a set of parallel or dependent transactions involve criminal proceeds if one such transaction does so.

Section 423: Suspension of Tax-Exempt Status of Designated Foreign Terrorist Organizations.

A group that the United States formally designates as a "terrorist organization" is liable, among many measures, to have their assets frozen and their members barred from entering the United States. However, under current law, "terrorist organizations" that have registered as tax-exempt organizations under section 501 of the Internal Revenue Code can retain their tax-exempt status. And individuals who contribute to these designated "terrorist organizations" still are able to deduct those contributions.

This section amends section 501 of the Internal Revenue Code to suspend automatically the tax exempt status of any group upon its designation as a "terrorist organization" under the several authorities. It also denies deductions for any donations made to such organizations during the period of suspension.

Section 424: Denial of Federal Benefits to Terrorists.

Current law allows federal courts to deny federal benefits to persons who have been convicted of drug-trafficking or drug-possession crimes. 21 U.S.C. § 862. As a result, these convicts can be prohibited, for periods of up to life, from receiving grants, contracts, loans, professional licenses, or commercial licenses that are provided by a federal agency or out of appropriated funds. But despite the fact that terrorism is at least as dangerous to the United States' national security as drug offenses, there presently is no legal authority to deny federal benefits to persons who have been convicted of terrorism crimes. This section would eliminate this inconsistency, and ensure that the same disincentives that the law creates with respect to drug crimes are available in the terrorism context, as well. Specifically, it would give federal courts the authority to deny federal benefits to any person convicted of an offense listed in 18 U.S.C. § 2332b(g)(5)(B).

Section 425: Corrections to Financing of Terrorism Statute.

This section corrects a number of drafting errors in the recently enacted financing of terrorism statute, 18 U.S.C. § 2339C, and supplies a definition for the term "material support or resources" as used in that statute by cross-referencing the existing definition in 18 U.S.C. § 2339A(b).

Section 426: Terrorism-related specified activities for money laundering.

This section adds three terrorism-related provisions to the list of specified unlawful activities that serve as predicates for the money laundering statute, 18 U.S.C. § 1956. Subsection (a) adds as a RICO predicate the offense in 18 U.S.C. § 1960 (relating to illegal money transmitting businesses), which has the effect of making this offense a money laundering predicate through the cross-reference in 18 U.S.C. § 1956(b)(7)(A). Subsection (b) directly adds as money laundering predicates the new terrorist-financing offense in 18 U.S.C. § 2339C and the offense of misusing social security numbers under 42 U.S.C. § 408.

Section 427: Assets of Persons Committing Terrorist Acts Against Foreign Countries or International Organizations.

The USA PATRIOT Act enacted a new forfeiture provision at 18 U.S.C. § 981(a)(1)(G) pertaining to the assets of any person planning or perpetrating an act of terrorism against the

United States. This section adds a parallel provision pertaining to the assets of any person planning or perpetrating an act of terrorism against a foreign state or international organization while acting within the jurisdiction of the United States.

Section 428: Technical and Conforming Amendments Relating to the USA PATRIOT Act.

This section makes a number of corrections relating to provisions of the USA PATRIOT Act, mostly affecting money laundering or asset forfeiture. While essentially technical in nature, these amendments are critical, because typographical and other errors in the USA PATRIOT Act provisions are preventing prosecutors from fully utilizing that Act's tools. For example, certain new forfeiture authorities enacted by that Act refer to a non-existent statute, 31 U.S.C. § 5333, where 31 U.S.C. § 5331 is intended.

Subsection (a) makes technical corrections to a number of provisions in the USA PATRIOT Act. Subsection (b) codifies section 316(a)-(c) of that Act as 18 U.S.C. § 987. Subsection (c) adds explicit language covering conspiracies to two offenses likely to be committed by terrorists (18 U.S.C. §§ 33 and 1366), conforming to section 811 of the USA PATRIOT Act, which added conspiracy language to other terrorism offense provisions.

Title V: Enhancing Immigration and Border Security

Section 501: Expatriation of Terrorists.

Under 8 U.S.C. § 1481, an American can lose his citizenship by voluntarily, and with the intent to relinquish nationality, taking any of a number of actions, including: (1) obtaining Nationality in a foreign state; (2) taking an oath of allegiance to a foreign state; and, most importantly, (3) serving in the armed forces of a foreign state that are engaged in hostilities against the United States. The current expatriation statute does not, however, provide for the relinquishing of citizenship in cases where an American serves in a hostile foreign terrorist organization. It thus fails to take account of the myriad ways in which, in the modern world, war can be waged against the United States.

This provision would amend 8 U.S.C. § 1481 to make clear that, just as an American can relinquish his citizenship by serving in a hostile foreign army, so can he relinquish his citizenship by serving in a hostile terrorist organization. Specifically, an American could be expatriated if, with the intent to relinquish nationality, he becomes a member of, or provides material support to, a group that the United States has designated as a "terrorist organization," if that group is engaged in hostilities against the United States.

This provision also would make explicit that the intent to relinquish nationality need not be manifested in words, but can be inferred from conduct. The Supreme Court already has recognized that intent can be inferred from conduct. *See, e.g.*, *Vance v. Terrazas*, 444 U.S. 252, 260 (1980) (recognizing that the "intent to relinquish citizenship . . . [can be] expressed in words or . . . found as a fair inference from proved conduct"); *see also King v. Rogers*, 463 F.2d 1188, 1189 (9th Cir. 1972) ("[S]pecific subjective intent to renounce United States citizenship . . . may [be] prove[d] . . . by evidence of an explicit renunciation, acts inconsistent with United States citizenship, or by affirmative voluntary act[s] clearly manifesting a decision to accept [foreign] nationality." (citations omitted)); *United States v. Schiffer*, 831 F. Supp. 1166, 1194 (E.D. Pa. 1993) ("Specific intent may . . . be proven by evidence of what steps the alleged expatriate did or did not take in connection with his expatriating acts."), *aff'd without opinion*, 31 F.3d 1175 (3rd Cir. 1994). Specifically, this proposal would make service in a hostile army or terrorist group prima facie evidence of an intent to renounce citizenship.

Section 502: Enhanced Criminal Penalties for Violations of Immigration and Nationality Act.

Aliens all too frequently flaunt the requirements of the Immigration and Nationality Act because that statute does not include effective criminal deterrence. There are minimal criminal penalties directly attached to fundamental violations, or there is no effective prosecution of fraudulent documents, marriage fraud, or unlawful employment of aliens. Criminal penalties in some cases are misdemeanors or require that a pattern and practice of violations be shown to warrant felony punishment. This provision would amend the INA to increase the penalties for a number of immigration crimes, including unlawful entries, alien-smuggling crimes, crimes involving fraud, and failures to depart.

Section 503: Inadmissibility and Removability of National Security Aliens or Criminally Charged Aliens.

The Attorney General does not have sufficient authority to bar an alien from the United States, or to remove an alien from the United States, on the basis of national security. The direct authority for barring admission or removing an alien does not provide sufficient authority for action based strictly on national security grounds. This provision would give the Attorney General sufficient authority to deny admission to the United States, or to remove from the United States, those individuals whom the Attorney General has reason to believe would pose a danger to the national security of the United States, based on the statutory definition of "national security" under the Act in connection with the designation of foreign terrorist organizations. The new ground of admissibility, and the new ground of removal, would parallel the authority currently granted to the Secretary of State in INA § 212(a)(3)(C)(i) to determine that an alien's entry or activities the Secretary has reasonable grounds to believe would have potentially serious adverse foreign policy consequences for the United States, thereby making the alien excludable.

In this case, the Attorney General must have reason to believe that the alien poses a danger to the national security of the United States and may deny admission. In addition, this provision would give the Attorney General the authority to bar from the United States aliens who have been convicted of, or charged with, serious crimes in other countries.

Section 504: Expedited Removal of Criminal Aliens.

Current law provides for the expedited removal of aliens in very limited circumstances. Expedited removal enables the government to quickly remove from the United States certain aliens who have been convicted of certain crimes, and renders the aliens ineligible for "discretionary relief." The expedited removal authorities (set forth in section 238(b) of the Immigration and Nationality Act, 8 U.S.C. § 1228(b)) only apply to nonpermanent resident aliens. In addition, only "aggravated felonies" can trigger expedited removal. But once an alien has been convicted of a criminal offense, any additional administrative process is unnecessary: a court has already found, beyond a reasonable doubt, that the alien has committed the acts which render him removable. Nor is there any reason to distinguish between aliens who are permanent residents and aliens who are not: for both types of aliens, the fact of a criminal conviction suffices to establish that a person is removable.

This provision would strengthen the existing expedited removal authorities in several ways. First, it would expand the individuals subject to expedited removal to include all aliens, not just nonpermanent residents. Second, it would expand the expedited-removal-triggering crimes to include some of the offenses listed in INA § 237(a)(2)(A), (B), (C) & (D), including possession of controlled substances, firearms offenses, espionage, sabotage, treason, threats against the President, violations of the Trading with the Enemy Act, draft evasion, and certain alien smuggling crimes. Perversely, many of these offenses are far more serious than "aggravated felonies," and yet at present do not trigger expedited removal.

In addition, this provision would curtail the authorities for contested judicial removal currently codified at INA § 238(c) (8 U.S.C. § 1228(c)). Contested judicial removal has been seldom utilized because its procedures are unduly cumbersome. They require the prosecutor and district judge to try immigration relief issues which are outside their areas of expertise—issues that particularly in the criminal context are properly committed to the Attorney General's discretion. The existing process also requires the INS Commissioner to make multiple submissions, once in presenting the immigration charges and basis, and then in responding to any relief request the aliens might make in the proceeding. The entire process significantly expands the scope of the criminal trial. The proposal to expand the streamlined administrative process to cover more aliens and more crimes would render contested judicial removal largely superfluous. This amendment would, however, preserve stipulated judicial orders as under existing subsection (c)(5). The amendment also would correct a technical error in the section numbering.

Section 505: Clarification of Continuing Nature of Failure-to-Depart Offense, and Deletion of Provisions on Suspension of Sentence.

The existing offense of failing to depart is defined in section 243(a)(1)(A) of the Immigration and Nationality Act (8 U.S.C. § 1253(a)(1)(A)). The statute applies to an alien's failure to depart "within a period of 90 days from the date of the final order." While this provision reasonably can be interpreted as a continuing offense, it is conceivable that aliens who have willfully remained in the United States for several years after a final order of removal might claim that prosecution is barred by the 5 year period of limitations. (18 U.S.C. § 3282).

This amendment would clarify existing law by making it explicit that a willful failure to depart is a continuing offense. Specifically, it would amend section 243(a)(1)(A) to expressly state that it is unlawful for any alien against whom a final order of removal is outstanding willfully to remain in the United States more than 90 days after the date of the final order of removal under administrative processes, or if judicial review is had, then more than 90 days after the final order of the court.

Subsection (b) of this proposal eliminates the authority of courts under 8 U.S.C. § 1253(a) to suspend for good cause the sentence of an alien convicted of failure to depart. This authority is inconsistent with the general principles of federal sentencing law, including the 1984 Sentencing Reform Act which, among other things, abolished suspension of sentence generally for federal offenses. The ability of courts to suspend sentences for failure to depart renders the potential criminal penalties for this offense ineffective. The Department does not expect that subsection (b) would be applied retroactively to offenders whose offenses occurred prior to the date of enactment.

Section 506: Additional Removal Authorities.

This section augments the specification of places to which aliens may be removed under 8 U.S.C. § 1231(b), to provide additional options where the alien cannot be removed to any country currently specified in the statute.