

**ANTI-TERRORISM ACT OF 2001**  
**SECTION -BY-SECTION ANALYSIS**

**Title I: Intelligence Gathering**

**Subtitle A: Electronic Surveillance**

**Section 101**                      **Modification of Authorities Relating to Use of Pen Registers And Trap  
And Trace Devices**

This section authorizes courts to grant pen register/trap and trace orders that are valid anywhere in the nation, and subjects Internet communications to the same rules as telephone communications. At present, the government must apply for new pen/trap orders in every jurisdiction where an investigation is being pursued. Hence, law enforcement officers tracking a suspected terrorist in multiple jurisdictions must waste valuable time and resources by obtaining a duplicative order in each jurisdiction.

In greater detail, the section amends 18 U.S.C. § 3123(a) by allowing courts to grant orders that are valid "anywhere within the United States." Thus, the government would be able to obtain one pen register/trap and trace order that could be applied to any communications provider in the chain of providers carrying the suspects' communications. This amendment would increase tracing efficiency by eliminating the current need to apply for new orders each time the investigation leads to another jurisdiction. The section also includes a number of provisions which ensure that the pen/trap provisions apply to facilities other than telephone lines (e.g., the Internet). These amendments will promote effective tracing regardless of the media employed.

**Section 102**                      **Seizure of Voice Mail Messages Pursuant to Warrants**

This section enables law enforcement personnel to seize suspected terrorists' voice mail messages pursuant to a search warrant. At present, 18 U.S.C. § 2510(1) anomalously defines "wire communication" to include "any electronic storage of such communication," meaning that the government must apply for a Title III wiretap order before it can obtain unopened voice mail messages held by a service provider. The section amends the definition of "wire communication" so that it no longer includes stored communications. It also amends 18 U.S.C. § 2703 to specify that the government may use a search warrant (instead of a wiretap order) to compel the production of unopened voicemail, thus harmonizing the rules applicable to stored voice and non-voice (e.g., e-mail) communications.

**Section 103**                      **Authorized Disclosure**

This section facilitates the disclosure of Title III information to other components of the intelligence community in terrorism investigations. At present, 18 U.S.C. § 2517(1) generally allows information obtained via wiretap to be disclosed only to the extent that it will assist a criminal investigation. One must obtain a court order to disclose Title III information in non-criminal proceedings. Section 109 would modify the wiretap statutes to permit the disclosure of Title III-generated information to a non-law enforcement officer for such purposes as furthering

an intelligence investigation. This will harmonize Title III standards with those of the Foreign Intelligence Surveillance Act (FISA), which allows such information-sharing. Allowing disclosure under Title III is particularly appropriate given that the requirements for obtaining a Title III surveillance order in general are more stringent than for a FISA order, and because the attendant privacy concerns in either situation are similar and are adequately protected by existing statutory provisions.

Section 104 Savings Provision

This provision clarifies that the collection of foreign intelligence information is governed by foreign intelligence authorities rather than by criminal procedural statutes, as the current statutory scheme envisions.

Section 105 Use of Wiretap Information From Foreign Governments

Under current case law, federal prosecutors appear to have the ability to use electronic surveillance conducted by foreign governments in criminal proceedings. As criminal law enforcement becomes more of a global effort, such information will come to play a larger role in federal prosecutions. To ensure uniformity of federal practice, this section codifies the principle that United States prosecutors may use against American citizens information collected by a foreign government even if the collection would have violated the Fourth Amendment. Under the proposal, such information may not be used if it was obtained with the knowing "participation" or at the direction of American law enforcement personnel, if gathered in violation of constitutional protections.

Section 106 Interception of Computer Trespasser Communications

Current law may not allow victims of computer trespassing to request law enforcement assistance in monitoring unauthorized attacks as they occur. Because service providers often lack the expertise, equipment, or financial resources required to monitor attacks themselves as permitted under current law, they often have no way to exercise their rights to protect themselves from unauthorized attackers. Moreover, such attackers can target critical infrastructures and engage in cyberterrorism. To correct this problem, and help to protect national security, the proposed amendments to the wiretap statute would allow victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems in a narrow class of cases.

Section 107 Scope of Subpoenas for Records of Electronic Communications

Current law allows the government to use a subpoena to compel communications providers to disclose a small class of records that pertain to electronic communications, limited to such records as the customer's name, address, and length of service. 18 U.S.C. § 2703(c)(1)(C). Remarkably, investigators cannot use a subpoena to obtain such records as credit card number or other form of payment. In many cases, users register with Internet service providers using false names, making the form of payment critical to determining the user's true

identity. Under current law, this information can only be obtained by the slower and more cumbersome process of a court order.

In fast-moving investigation such as terrorist bombings – in which Internet communications are critical method of identifying conspirators in determining the source of the attacks -- the delay necessitated by the use of court orders can often be important. Obtaining billing and other information can identify not only the perpetrator but also give valuable information about the financial accounts of those responsible and their conspirators. Therefore, the proposed amendments to § 2703(c)(1)(C) would update and broaden the class of records that law enforcement authorities may obtain with a subpoena.

Section 108                      Nationwide Service of Search Warrants for Electronic Evidence

Current law requires the government to use a search warrant to compel a provider to disclose unopened e-mail. 18 U.S.C. § 2703(a). Because Federal Rule of Criminal Procedure 41 requires that the “property” to be obtained be “within the district” of the issuing court, however, the rule may not allow the issuance of § 2703(a) warrants for e-mail located in other districts. Thus, for example, where an investigator in Boston is seeking electronic e-mail in the Yahoo! account of a suspected terrorist, he may need to coordinate with agents, prosecutors, and judges in the Northern District of California, none of whom have any other involvement in the investigation. This electronic communications information can be critical in establishing relationships, motives, means, and plans of terrorists. Moreover, it is equally relevant to cyber-incidents in which a terrorist motive has not (but may well be) identified. Finally, even cases that require the quickest response (kidnappings, threats, or other dangers to public safety or the economy) may rest on evidence gathered under § 2703(a). To further public safety, this section accordingly authorizes courts with jurisdiction over investigations to compel evidence directly, without requiring the intervention of their counterparts in the districts where major Internet service providers are located.

Section 109                      Clarification of Scope

Law enforcement must have the capability to trace, intercept, and obtain records of the communications of terrorists and other criminals with great speed, even if they choose to use a cable provider for their telephone and Internet service. This section amends the Cable Communications Policy Act (“Cable Act”) to clarify that when a cable company acts as a telephone company or an Internet service provider, it must comply with the same laws governing the interception and disclosure of wire and electronic communications that apply to any other telephone company or Internet service provider. The Cable Act, passed in 1984 to regulate various aspects of the cable television industry, could not take into account the changes in technology that have occurred over the last seventeen years. Cable television companies now often provide Internet access and telephone service in addition to television programming. Because of perceived conflicts between the Cable Act and the laws that govern law enforcement’s access to communications and records of communications carried by cable companies, cable providers have refused to comply with lawful court orders, thereby slowing or ending critical investigations.

Section 110                      Emergency Disclosure of Electronic Communications

Existing law contains no provision that allows providers of electronic communications service to disclose the communications (or records relating to such communications) of their customers or subscribers in emergencies that threaten death or serious bodily injury. This section amends 18 U.S.C. § 2702 to authorize such disclosures if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.

Current law also contains an odd disconnect: a provider may disclose the contents of the customer's communications in order to protect its rights or property but the current statute does not expressly permit a provider to voluntarily disclose non-content records (such as a subscriber's login records). 18 U.S.C. § 2702(b)(5). This problem substantially hinders the ability of providers to protect themselves from cyber-terrorists and criminals. Yet the right to disclose the contents of communications necessarily implies the less intrusive ability to disclose non-content records. In order to promote the protection of our nation's critical infrastructures, this section's amendments allow communications providers to voluntarily disclose both content and non-content records to protect their computer systems.

Subtitle B: Foreign Intelligence Surveillance

Section 151                      Period of Orders of Electronic Surveillance of Non-United States Persons Under Foreign Intelligence Surveillance

This section reforms a critical aspect of the Foreign Intelligence Surveillance Act (FISA). It will enable the Foreign Intelligence Surveillance Court (FISC), which presides over applications made by the U.S. government under FISA, to authorize the search and surveillance in the U.S. of officers and employees of foreign powers and foreign members of international terrorist groups for up to a year. Currently, the FISC may only authorize such searches and surveillance for up to 45 days and 90 days, respectively. The proposed change would bring the authorization period in line with that allowed for search and surveillance of the foreign establishments for which the foreign officers and employees work. **The proposed change would have no effect on electronic surveillance or physical searches of U.S. citizens or permanent**

resident aliens.

Section 152                    Multi-Point Authority

This provision expands the obligations of third parties to furnish assistance to the government under FISA. Under current FISA provisions, the government can seek information and assistance from common carriers, landlords, custodians and other persons specified in court-ordered surveillance. Section 152 would amend FISA to expand existing authority to allow, "in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person," that a common carrier, landlord, custodian or other person not specified in the Court's order be required to furnish the applicant information and technical assistance necessary to accomplish electronic surveillance in a manner that will protect its secrecy and produce a minimum of interference with the services that such person is providing to the target of electronic surveillance. This would enhance the FBI's ability to monitor international terrorists and intelligence officers who are trained to thwart surveillance by rapidly changing hotel accommodations, cell phones, Internet accounts, etc., just prior to important meetings or communications. Under the current law, the government would have to return to the FISA Court for an order that named the new carrier, landlord, etc., before effecting surveillance. Under the proposed amendment, the FBI could simply present the newly discovered carrier, landlord, custodian, or other person with a generic order issued by the Court, and could then effect FISA coverage as soon as technically feasible.

Section 153                    Foreign Intelligence Information

Current law requires that FISA be used only where foreign intelligence gathering is the sole or primary purpose of the investigation. This section will clarify that the certification of a FISA request is supportable where foreign intelligence gathering is "a" purpose of the investigation. This change would eliminate the current need continually to evaluate the relative weight of criminal and intelligence purposes, and would facilitate information sharing between law enforcement and foreign intelligence authorities which is critical to the success of anti-terrorism efforts.

Section 154                    Foreign Intelligence Information Sharing

With limited exceptions, it is presently impossible for criminal investigators to share information obtained through a grand jury (including through the use of grand jury subpoenas) and information obtained from electronic surveillance authorized under Title III with the intelligence community. This limitation will be very significant in some criminal investigations. For example, grand jury subpoenas often are used to obtain telephone, computer, financial, and other business records in organized crime investigations. Thus, these relatively basic investigative materials are inaccessible for examination by intelligence community analysts working on related transnational organized crime groups. A similar problem occurs in computer

intrusion investigations: grand jury subpoenas and Title III intercepts are used to collect transactional data and to monitor the unknown intruders. The intelligence community will have an equal interest in such information, because the intruder may be acting on behalf of a foreign power.

Section 155 Pen Register And Trap And Trace Authority

When added to FISA two years ago, the pen register/trap and trace section was intended to mirror the criminal pen/trap authority defined in 18 U.S.C. § 3123. In fact, the FISA authority differs from the criminal authority only in that it requires, in addition to a showing of relevance, an additional factual showing that the communications device has been used to contact an "agent of a foreign power" engaged in international terrorism or clandestine intelligence activities. This has the effect of making the FISA pen/trap authority much more difficult to obtain. In fact, the process for obtaining FISA pen/trap authority is only slightly less burdensome than the process for obtaining full electronic surveillance authority under FISA. This stands in stark contrast to the criminal pen/trap authority, which can be obtained quickly from a local court, on the basis of a certification that the information to be obtained is relevant to an ongoing investigation. The amendment simply eliminates the "agent of a foreign power" prong from the predication, and thus makes the FISA authority more closely track the criminal authority.

Section 156 Business Records

\_\_\_\_\_The "business records" section of FISA (50 U.S.C. §§ 1861 and 1862) requires a formal pleading to the Court and the signature of a FISA judge (or magistrate). In practice, this makes the authority unavailable for most investigative contexts. The time and difficulty involved in getting such pleadings before the Court usually outweighs the importance of the business records sought. Since its enactment, the authority has been sought less than five times. This section would delete the old authority and replace it with a generic "administrative subpoena" authority for documents and records. This authority, modeled on the administrative subpoena authority available to drug investigators pursuant to Title 21, allows the Attorney General to compel production of such records upon a finding that the information is relevant.

Section 157 Miscellaneous National Security Authorities

At the present time, National Security Letter (NSL) authority exists in three separate statutes: the Electronic Communications Privacy Act (for telephone and electronic communications records), the Financial Right to Privacy Act (for financial records), and the Fair Credit Reporting Act (for credit records). Like the FISA pen register/trap and trace authority described above, NSL authority requires both a showing of relevance and a showing of links to an "agent of a foreign power." In this respect, they are substantially more demanding than the analogous criminal authorities, which require only a certification of relevance. Because the NSLs require documentation of the facts supporting the "agent of a foreign power" predicate and because they require the signature of a high-ranking official at FBI headquarters, they often take months to be issued. This is in stark contrast to criminal subpoenas, which can be used to obtain

the same information, and are issued rapidly at the local level. In many cases, counterintelligence and counterterrorism investigations suffer substantial delays while waiting for NSLs to be prepared, returned from headquarters, and served. The section would streamline the process of obtaining NSL authority, and also clarify that the FISA Court can issue orders compelling the production of consumer reports.

Section 158                      Disclosure of Educational Records

The Department believes that there may be information contained in student education records maintained by educational agencies and institutions and in education surveys reported to the National Center for Education Statistics that could be important in the criminal investigation of the terrorist attack of September 11, 2001, as well as to national security. However, section 408 of the National Statistics Act clearly prohibits disclosure of such information to appropriate Federal officials for these purposes; and, of equal importance, section 408 criminalizes the disclosure of any such prohibited information. This section will effectively override section 408 for this limited purpose.

Section 444 (Protection of the Rights and Privacy of Students and Parents, commonly referred to as FERPA) of the General Education Provisions Act generally prohibits the release of personally identifiable information from student education records without the consent of the student (or, in the case of a minor, the student's parents). While there are certain exceptions to this prohibition, it is not clear that these exceptions are fully applicable to the pressing need to share such information from student education records relating to terrorism with the appropriate Federal officials for the purpose of criminal investigation and prosecution and ensuring national security. This section will effectively override section 444 for this limited purpose.

Section 159                      Presidential Authorities

This section is designed to accomplish two principal objectives. First, the section restores to the President, in limited circumstances involving armed hostilities or attacks against the United States, the power to confiscate and vest in the United States the property of enemies during times of national emergency, which was contained in the Trading with the Enemy Act, 50 app. U.S.C. sect. 5(b) (TWEA) until 1977. Until the International Economic Emergency Act (IEEPA) was passed in 1977, section 5(b) permitted the President to vest enemy property in the United States during time of war *or* national emergency. When IEEPA was passed, it did not expressly include a provision permitting the vesting of property in the United States, and section 5(b) of TWEA was amended to apply only "[d]uring the time of war." 50 app. U.S.C. sect. 5(b).

This new provision tracks the vesting language currently in section 5(b) of TWEA and permits the President, only in the limited circumstances when the United States is engaged in military hostilities or has been subject to an attack, to confiscate property of any foreign country, person, or organization involved hostilities or attacks on the United States. Like the original provision in TWEA, it is an exercise of Congress's war power under Article I, section 8, clause 11 of the Constitution and is designed to apply to unconventional warfare where Congress has not formally declared war against a foreign nation.

The second principal purpose of this amendment to IEEPA is to ensure that reviewing courts may base their rulings on an examination of the complete administrative record in sensitive national security or terrorism cases without requiring the United States to compromise classified information.

New subsection (c) would authorize a reviewing court, in the process of verifying that determinations made by the executive branch were based upon substantial evidence and were not arbitrary or capricious, to consider classified evidence ex parte and in camera. This would ensure that

reviewing courts have the best and most complete information upon which to base their decisions without forcing the United States to choose between compromising highly sensitive intelligence information or declining to take action against individuals or entities that may present a serious threat to the United States or its nationals. A similar accommodation mechanism was enacted by Congress in the Anti-Terrorism and Effective Death Penalty Act of 1996, 8 U.S.C. Section 1189(b)(2).

## **TITLE II: IMMIGRATION**

### Section 201                      Definitions Relating to Terrorism

The Alien Terrorist Removal Court is the only mechanism available to the government in which classified evidence can be used as part of an affirmative case to remove an alien involved in terrorism. In existence since 1996, it has never been used, in part because of the narrow definition of "terrorist" which limits the applicability of the Court. The current definition is limited to individuals who provide material support for a "terrorist activity." This section broadens that definition to include anyone who affords material support to an organization that the individual knows or should know is a terrorist organization, regardless of whether or not the purported purpose for the support is related to terrorism. These revised definitions will apply in all types of removal proceedings (before the Alien Terrorist Removal Court, immigration courts, and the INS). This legislation seeks to stop the provision of support to terrorist organizations through sham non-terrorist activities. The legislation further defines terrorist organization and provides a mechanism for the designation and redesignation of groups as terrorist organizations.

### Section 202                      Mandatory Detention of Suspected Terrorists

Currently, persons deportable or inadmissible for terrorism-related reasons must be detained. This section expands this mandatory detention to those individuals the Attorney General determines pose a threat to national security, whether or not the alien is eligible for or is granted relief from removal. The Attorney General is vested with the discretion to make these time-sensitive decisions and to detain individuals who are found to pose a threat to national security until they are actually removed or until the Attorney General determines the person no longer poses a threat.

### Section 203                      Habeas Corpus and Judicial Review

Under current law, determinations to remove or detain terrorists have generally been deemed by the courts to be reviewable by habeas corpus proceedings which can be brought in

any applicable federal jurisdiction nationwide. The availability of multiple jurisdictions for review creates the potential for inconsistent standards to be developed by reviewing courts, which interferes with the government's ability to pursue detention and removal under a known and consistent standard. The proposed provision would not limit the scope of judicial review, but would vest exclusive judicial review of detention and removal proceedings with respect to aliens certified by the Attorney General as national security risks in the federal courts for the District of Columbia. The reservation of all alien terrorist cases to the District of Columbia conforms to general principles of administrative law, and to the existing provisions of the Immigration and Nationality Act. It is common for judicial review of agency action to be confined to a single court, and the Immigration and Nationality Act already limits challenges to expedited removal and Alien Terrorist Removal Court cases to the District of Columbia.

Section 204                      Applicability

This provision makes it clear that this legislation will apply to all aliens regardless of when they entered the United States or when they committed the terrorist activity.

Section 205                      Multilateral Cooperation Against Terrorists

This section will enhance our ability to combat terrorism and crime worldwide by providing new exceptions to the laws regarding disclosure of information from visa records. Under current law the Secretary of State may only disclose such information when doing so is directly related to the administration or enforcement of U.S. laws or a court makes the request. Often these showings are difficult to make in responding to an information request from a foreign government due to constraints of time or foreign procedure which preclude the involvement of a foreign court. This section grants the Secretary of State discretion to provide such information to foreign officials on a case-by-case basis for the purpose of fighting international terrorism or crime. It would also allow the Secretary to provide countries with which he negotiates specific agreements to have more general access to information from the State Department's lookout databases where the country will use such information only to deny visas to persons seeking to enter its territory.

Section 206                      Interagency Data Sharing

This amendment to the Immigration and Nationality Act (INA) would recognize that the interagency cooperation provided for in INA Section 105 now serves a broader border security function, and would enhance that function by improving consular officers' access to crime information. This is consistent with the fact that securing the borders of the U.S. against the entry of international terrorists, traffickers in narcotics, weapons or persons, international organized crime members, and illegal entrants is not the responsibility of any single federal agency. Consular officers abroad must facilitate legitimate travel while preventing the travel of individuals who present security or other threats to U.S. government interests. These officers need electronic access to information from border security and law enforcement agencies that will assist in identifying high-risk travelers, including information maintained by the FBI on aliens suspected of committing crimes in the U.S. (*e.g.*, information contained in the NCIC-III

and Wanted Persons File databases). Without this information, a consular officer could unknowingly grant a visa to a known or suspected criminal.

### **TITLE III – CRIMINAL JUSTICE**

#### **Subtitle A: Substantive Criminal Law**

##### **Section 301 No Statute of Limitations For Prosecuting Terrorism Offenses**

This section amends 18 U.S.C. § 3286 to provide that terrorism offenses may be prosecuted without limitation of time. This will make it possible to prosecute the perpetrators of terrorist acts whenever they are identified and apprehended.

The section expressly provides that it is applicable to offenses committed before the date of enactment of the statute, as well as those committed thereafter. This retroactivity provision ensures that no limitation period will bar the prosecution of crimes committed in connection with the September 11, 2001 terrorist attacks. The constitutionality of such retroactive applications of changes in statutes of limitations is well-settled. See, e.g., United States v. Grimes, 142 F.3d 1342, 1350-51 (11th Cir. 1998); People v. Frazer, 982 P.2d 180 (Cal. 1999).

Existing federal law (18 U.S.C. § 3282) bars prosecuting most offenses after five years. 18 U.S.C. § 3286, as currently formulated, extends the limitation period for prosecution for certain offenses that may be committed by terrorists – but only to eight years. While this is a limited improvement over the five-year limitation period for most federal offenses, it is patently inadequate in relation to the catastrophic human and social costs that frequently follow from such crimes as destruction of aircraft (18 U.S.C. § 32), aircraft hijackings (42 U.S.C. §§ 46502, 46504-06), attempted political assassinations (18 U.S.C. §§ 351, 1116, 1751), or hostage taking (18 U.S.C. § 1203). These are not minor acts of misconduct which can properly be forgiven or forgotten merely because the perpetrator has avoided apprehension for some period of time. Anomalously, existing law provides longer limitation periods for such offenses as bank frauds and certain artwork thefts (18 U.S.C. §§ 3293-94) than it does for the crimes characteristically committed by terrorists.

In many American jurisdictions, the limitation periods for prosecution for serious offenses are more permissive than those found in federal law, including a number of states which have no limitation period for the prosecution of felonies generally. While this section does not go so far, it does eliminate the limitation period for prosecution of the major crimes that are most likely to be committed by terrorists (“Federal terrorism offenses”), as specified in section 310 of this bill.

##### **Section 302 Alternative Maximum Penalties For Terrorism Crimes**

Under existing law, the maximum prison terms for federal offenses are normally determined by specifications in the provisions which define them. These provisions can provide inadequate maxima in cases where the offense is aggravated by its terrorist character or motivation. This section accordingly adds a new subsection (e) to 18 U.S.C. § 3559 which provides alternative maximum prison terms, including imprisonment for any term of years or for

life, for crimes that are likely to be committed by terrorists. This is analogous to the maximum fine provisions of 18 U.S.C. § 3571(b)-(c) – which supersede lower fine amounts specified in the statutes defining particular offenses – and will more consistently ensure the availability of sufficiently high maximum penalties in terrorism cases. As in several other provisions of this bill, the list of the serious crimes most frequently committed by terrorists set forth in section 310 of the bill (“Federal terrorism offenses”) is used in defining the scope of the provision.

This section affects only the maximum penalty allowed by statute. It does not limit the authority of the Sentencing Commission and the courts to tailor the sentences imposed in particular cases to offense and offender characteristics.

### Section 303                      Penalties For Terrorist Conspiracies

The maximum penalty under the general conspiracy provision of federal criminal law (18 U.S.C. § 371) is five years, even if the object of the conspiracy is a serious crime carrying a far higher maximum penalty. For some individual offenses and types of offenses, special provisions authorize conspiracy penalties equal to the penalties for the object offense – see, e.g., 21 U.S.C. § 846 (drug crimes) – but there is no consistently applicable provision of this type for the crimes that are likely to be committed by terrorists.

This section accordingly adds a new § 2332c to the terrorism chapter of the criminal code – parallel to the drug crime conspiracy provision in 21 U.S.C. § 846 – which provides maximum penalties for conspiracies to commit terrorism crimes that are equal to the maximum penalties authorized for the objects of such conspiracies. This will more consistently provide adequate penalties for terrorist conspiracies. As in various other provisions in this bill, the relevant class of offenses is specified by use of the notion of “Federal terrorism offense,” which is defined in section 310 of the bill.

### Section 304                      Terrorism Crimes as Rico Predicates

The list of predicate federal offenses for RICO, appearing in 18 U.S.C. § 1961(1), includes none of the offenses which are most likely to be committed by terrorists. This section adds terrorism crimes to the list of RICO predicates, so that RICO can be used more frequently in the prosecution of terrorist organizations. As in various other provisions, the list of offenses in section 309 of the bill (“Federal terrorism offenses”) is used in identifying the relevant crimes.

### Section 305                      Biological Weapons

Current law prohibits the possession, development, acquisition, etc., of biological agents or toxins “for use as a weapon.” 18 U.S.C. § 175. This section amends the definition of “for use as a weapon” to include all situations in which it can be proven that the defendant had any purpose other than a prophylactic, protective, or peaceful purpose. This will enhance the government’s ability to prosecute suspected terrorists in possession of biological agents or toxins, and conform the scope of the criminal offense in 18 U.S.C. § 175 more closely to the related forfeiture provision in 18 U.S.C. § 176. Moreover, the section adds a subsection to 18 U.S.C. § 175 which defines an additional offense of possessing a biological agent or toxin of a

type or in a quantity that, under the circumstances, is not reasonably justified by a prophylactic, protective or other peaceful purpose. The section also enacts a new statute, 18 U.S.C. § 175b, which generally makes it an offense for a person to possess a listed biological agent or toxin if the person is disqualified from firearms possession under 18 U.S.C. § 922(g).

The section further provides that the Department of Health and Human Services enhance its role in bioterrorism prevention by requiring registration of all research and public health laboratories and manufacturing facilities that possess certain hazardous microorganisms and toxins (the “Select Agents”) that have a high national security risk; requiring all such registered laboratories and manufacturing facilities to meet regulatory standards regarding the physical environment within which such Select Agents are maintained or used; specifying the qualifications of individuals authorized to work with such Select Agents; and specifying the institutional procedures for access to such Select Agents or the facilities in which they are maintained or used.

Section 306 Support of Terrorism Through Expert Advice or Assistance

18 U.S.C. § 2339A prohibits providing material support or resources to terrorists. The existing definition of “material support or resources” is generally not broad enough to encompass expert services and assistance – for example, advice provided by a person with expertise in aviation matters to facilitate an aircraft hijacking, or advice provided by an accountant to facilitate the concealment of funds used to support terrorist activities. This section accordingly amends 18 U.S.C. § 2339A to include expert services and assistance, making the offense applicable to experts who provide services or assistance knowing or intending that the services or assistance is to be used in preparing for or carrying out terrorism crimes. The section also amends 18 U.S.C. § 2339A to conform its coverage of terrorism crimes to the more complete list specified in section 309 of the bill (“federal terrorism offenses”).

Section 307 Prohibition Against Harboring Terrorists

18 U.S.C. § 792 makes it an offense to harbor or conceal persons engaged in espionage. There is no comparable provision for terrorism, though the harboring of terrorists creates a risk to the nation readily comparable to that posed by harboring spies. This section accordingly amends 18 U.S.C. § 792 to make the same prohibition apply to harboring or concealing persons engaged in federal terrorism offenses (as defined in section 309 of the bill).

Section 308 Post-Release Supervision of Terrorists

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

This section accordingly adds a new subsection to 18 U.S.C. § 3583 to authorize longer supervision periods, including potentially lifetime supervision, for persons convicted of terrorism crimes. This would permit appropriate tracking and oversight following release of offenders whose involvement with terrorism may reflect lifelong ideological commitments. As in other provisions in this bill, the covered class of crimes is federal terrorism offenses, which are specified in section 310 of the bill.

This section affects only the maximum periods of post-release supervision allowed by statute. It does not limit the authority of the Sentencing Commission and the courts to tailor the supervision periods imposed in particular cases to offense and offender characteristics, and the courts will retain their normal authority under 18 U.S.C. § 3583(e)(1) to terminate supervision if it is no longer warranted.

Section 309                      Definition

This section adds a new § 25 to title 18 of the United States Code, which defines the term “Federal terrorism offense.” The term is used in various provisions in this bill. The definition is designed to cover the major crimes which are most frequently involved in or associated with terrorism. The definition in the new 18 U.S.C. § 25 is largely based on an existing listing of terrorism-related offenses in 18 U.S.C. § 2332b(g)(5)(B).

Subtitle B – Criminal Procedure

Section 351                      Single-Jurisdiction Search Warrants For Terrorism

Rule 41(a) of the Federal Rules of Criminal Procedure currently requires a search warrant to be obtained within a district for searches within that district. The only exception is for cases in which the property or person is presently within the district but might leave the district before the warrant is executed.

The restrictiveness of the existing rule creates unnecessary delays and burdens for the government in the investigation of terrorist activities and networks that span a number of districts, since warrants must be separately obtained in each district. This section resolves that problem by providing that warrants can be obtained in any district in which activities related to the terrorism may have occurred, regardless of where the warrants will be executed.

Section 352                      Notice

The law that currently governs notice to subjects of warrants, where there is a showing to the court that immediate notice would jeopardize an ongoing investigation or otherwise interfere with lawful law-enforcement activities, is a mix of inconsistent rules, practices, and court decisions varying widely from jurisdiction to jurisdiction across the country. This greatly hinders the investigation of many terrorism cases and other cases.

This section resolves this problem by establishing a statutory, uniform standard for all such circumstances. It incorporates by reference the familiar, court-enforced standards currently

applicable to stored communications under 18 U.S.C. § 2705, and applies them to all instances where the court is satisfied that immediate notice of execution of a search warrant would jeopardize an ongoing investigation or otherwise interfere with lawful law-enforcement activities.

Section 353                      DNA Identification of Terrorists

The statutory provisions governing the collection of DNA samples from convicted federal offenders (42 U.S.C. § 14135a(d)) are restrictive, and do not include persons convicted for the crimes that are most likely to be committed by terrorists. DNA samples cannot now be collected even from persons federally convicted of terrorist murders in most circumstances. For example, 49 U.S.C. § 46502, which applies to terrorists who murder people by hijacking aircraft, 18 U.S.C. § 844(i), which applies to terrorists who murder people by blowing up buildings, and 18 U.S.C. § 2332, which applies to terrorists who murder U.S. nationals abroad, are not included in the qualifying federal offenses for purposes of DNA sample collection under existing law. This section addresses the deficiency of the current law in relation to terrorists by extending DNA sample collection to all persons convicted of terrorism crimes.

Section 354                      Grand Jury Matters

This section makes changes in Rule 6(e) of the Federal Rules of Criminal procedure, relating to grand jury secrecy, to address three problems. First, in national security and terrorism cases, the amendment permits sharing of grand-jury information to intelligence and national-defense personnel in terrorism and national-security cases. Second, the amendment permits the distribution of grand-jury information to law-enforcement personnel without the current requirement of providing the judge supervising the grand jury with a list of the names of every agent receiving the information. This requirement can be very impractical in such cases; the current investigation involves thousands of investigative agents. Third, the amendment clarifies that "matters occurring before the grand jury" does not include pre-existing subpoenaed documents and the like. While a number of courts of appeals have already adopted this interpretation, some courts have taken a contrary view, inhibiting distribution of such items to investigators in nationwide cases.

Section 355                      Extraterritoriality

Under existing law, some terrorism crimes have extraterritorial applicability, and can be prosecuted by the United States regardless of where they are committed – for example, offenses occurring outside the boundaries of the United States (see, for example, 18 U.S.C. §§ 175 (biological weapons offense), 2332a (use of weapons of mass destruction), and 2332b (terrorism transcending national boundaries)). However, there are no explicit extraterritoriality provisions in the statutes defining many other offenses which are likely to be committed by terrorists. This section helps to ensure that terrorist acts committed anywhere in the world can be effectively prosecuted by specifying that there is extraterritorial jurisdiction for the prosecution of all federal terrorism offenses.

Section 356                      Definition.

This amendment would explicitly extend the special and maritime criminal jurisdiction of the United States to U.S. diplomatic and consular premises and related private residences overseas, to the extent an offense is committed by or against a U.S. national. When offenses are committed by or against a U.S. national abroad on U.S. government property, the country in which the offense occurs may have little interest in prosecuting the case. Unless the United States is able to prosecute such offenders, these crimes may go unpunished. This section clarifies inconsistent caselaw to establish that the United States may prosecute offenses committed in its missions abroad, by or against its nationals.

**TITLE IV – FINANCIAL INFRASTRUCTURE**

Section 401                      Laundering The Proceeds of Terrorism.

Money-laundering under 18 U.S.C. § 1956 involves conducting or attempting to conduct a financial transaction knowing that the property involved represents the proceeds of an unlawful activity specified in subsection (c)(7) of the statute. Violations of 18 U.S.C. § 2339A, which prohibits providing material support to terrorists within the United States, are already included as specified unlawful activities. This section provides more complete coverage of money-laundering related to terrorism by adding as a further predicate offense 18 U.S.C. § 2339B, which prohibits providing material support or resources to foreign terrorist organizations.

Section 402                      Material Support For Terrorism

18 U.S.C. § 2339A prohibits providing material support to terrorism. Under the statute's definitional subsection, the prohibited forms of support include (among many other things) "currency or other financial securities." This section adds an explicit reference to "monetary instruments" to the definition. The purpose of the amendment is to make it clear that the definition is to be taken expansively to encompass any and all forms of money, monetary instruments, or securities.

Section 403                      Assets of Terrorist Organizations

Current law does not contain any authority tailored specifically to the confiscation of terrorist assets. Instead, currently, forfeiture is authorized only in narrow circumstances for the proceeds of murder, arson, and some terrorism offenses, or for laundering the proceeds of such offenses. However, most terrorism offenses do not yield "proceeds," and available current forfeiture laws require detailed tracing that is quite difficult for accounts coming through the banks of countries used by many terrorists.

This section increases the government's ability to strike at terrorist organizations' economic base by permitting the forfeiture of its property regardless of the source of the property, and regardless of whether the property has actually been used to commit a terrorism offense. This is similar in concept to the forfeiture now available under RICO. In parity with the drug forfeiture laws, Section 403 also authorizes the forfeiture of property used or intended to be used to

facilitate a terrorist act, regardless of the source of the property. There is no need for a separate criminal forfeiture provision because criminal forfeiture is incorporated under current law by reference. The provision is retroactive to permit it to be applied to the events of September 11, 2001.

Section 404                      Technical Clarification Relating to Provision of Material Support to  
Terrorism

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

Section 405                      Disclosure of Tax Information in Terrorism And National-Security  
Investigations

Taxpayer records maintained by the Internal Revenue Service (IRS) are subject to strict rules regarding disclosure to other Government agencies, detailed in 26 U.S.C. § 6103. Although the law currently allows for the disclosure of such information to non-Treasury personnel in emergency circumstances, there is no terrorism-specific exception. This section amends § 6103 to permit disclosure of IRS-maintained information to Federal, State and local law enforcement agencies who are part of a joint investigative team with the Federal agency.

There is currently no mechanism for the release of tax information to Department of Justice personnel involved in counterterrorism investigations, nor a mechanism to allow those Treasury Department components involved in counterterrorism analysis to disseminate such information to the intelligence community. This section amends § 6103 to allow for the release of tax information to Department of Justice and Department of Treasury personnel involved in counterterrorism investigations and analysis, and to permit this information to be disseminated to the intelligence community.

Section 406                      Restraint of Property Subject to Criminal Forfeiture

Following the conviction in a criminal case, a court may order the forfeiture of property traceable to the offense, or it may enter a judgment in favor of the government for the value of that property if the traceable property is unavailable. *United States v. Candelaria-Silva*, 166 F.3d 19 (1st Cir. 1999) (criminal forfeiture order may take several forms: money judgment, directly forfeitable property, and substitute assets). To make such post-conviction remedies effective, it is necessary for the court to be able to restrain assets pre-trial so that they are available, in the event of conviction, to satisfy the forfeiture judgment.

This section slightly expands the scope of the property that may be restrained pre-trial to ensure that there are sufficient assets to satisfy a judgment. Although some courts interpret current law to allow pre-trial restraint of non-traceable assets, see *In Re Billman*, 915 F.2d 916 (4th Cir. 1990), others only permit the government to restrain assets themselves traceable to the offense, see *United States v. Gotti*, 155 F.3d 144 (2d Cir. 1998). The proposed amendment would recognize that many assets are "fungible," and assist the government's ability to deprive terrorists of their assets without proving the assets they are able to locate are themselves traceable to the offense. Without this amendment, in courts that take the narrower view of the law, the government is unable to preserve the assets of major crime figures during the trial to ensure that they are available to satisfy a judgment in the event of a conviction. See *Gotti, supra* (vacating pre-trial order restraining assets of organized crime leader).

This section would permit pretrial restraint of substitute assets only in criminal forfeiture cases, and only after a grand jury has found probable cause to believe an offense giving rise to a forfeiture has been committed. The property can actually be forfeited to the government only after a petit jury has found the offense proved beyond a reasonable doubt and returned a judgment of conviction. The amendment is made to the Controlled Substances Act because the provisions governing criminal forfeitures in drug cases are incorporated, by statute, into all other criminal forfeiture statutes. 28 U.S.C. §2461(c).

Section 407                      Trade Sanctions Reform Act of 2000

The Trade Sanctions Reform Act of 200 requires the President to end unilateral agricultural and medical sanctions with respect to foreign entities and governments. The section would authorize Presidential control of agricultural and medical exports to all designated terrorists and narcotics entities wherever they are located. The section would authorize the President to retain sanctions with respect to exports of agricultural commodities, medicine and medical devices to designated terrorist entities.

Section 408                      Extraterritorial Jurisdiction

Financial crimes admits of no border, utilizing the integrated global financial network for ill purposes. This provision would apply the financial crimes prohibitions to conduct committed abroad, so long as the tools or proceeds of the crimes passes through or are in the United States.

**TITLE V – EMERGENCY AUTHORIZATIONS**

Section 501                      Office of Justice Programs

This provision provides benefits to public safety officers disabled as a result of the September 11 attacks, as well as grants to the States for victim assistance. Consistent with 42 U.S.C. § 3796(b), the Department of Justice's FY2001 appropriations act places an aggregate cap of \$2.4 million on the benefits that may be paid to public safety officers who have become totally disabled. A similar cap is found in both House and Senate FY2002 bills. Section 501 removes all caps with respect to officers who were totally disabled as a result of the September 11 attacks. This would authorize OJP annually to pay approximately \$120,000 to each totally-disabled officer for life or while he remains totally disabled. In the same way, the Department of

Justice's existing grant programs to assist States in aiding crime victims provide mechanisms to respond to the attacks, 42 U.S.C. § 10603b, but the amounts available to meet the need are insufficient. Section 501 would authorize the spending of up to \$700 million from balances in the Crime Victims Fund (currently \$1.4 billion) to assist States in their victim-relief efforts. The \$700 million could be dispatched almost immediately to the States affected by the terrorist attacks, providing them with resources to supplement their own expenditures in aid of the victims.

Current law limits OJP's authority to work directly with service providers (as opposed to governments) under the circumstances created by the September 11 attacks, and to coordinate and manage emergency-response and other activities of its various components. 42 U.S.C. § 10603b(b). The law also is unclear as to proper execution of certain aspects of the Public Safety Officers Benefits program. Section 501 would amend OJP's authorities in these areas, specifically by authorizing OJP to work directly with service providers, in addition to governmental entities, to expedite terrorism victim relief efforts, by enhancing its authority to coordinate and manage emergency-response and other activities of its various components, and by clarifying provisions governing the provision of public safety officer benefits.

Section 502 Attorney General's Authority to Pay Rewards

Section 106 of the FY2001 DOJ appropriations act places a per-reward cap of \$2 million (and a \$10 million annual aggregate cap) on rewards that the Attorney General may offer. A similar cap is found in both House and Senate FY2002 bills. Given the increasing sophistication of terrorist acts, these limitations may hamper the Justice Department's ability to bring the guilty to justice. Section 502 therefore would remove these caps. It would authorize the Attorney General to offer or pay rewards of any amount he or the President determines to be necessary for information or assistance.

Section 503 Limited Authority to Pay Overtime

For the past several years the Department of Justice Appropriations Acts have included provisions whereby Immigration and Naturalization Service funds could not be used to pay employees overtime pay in an amount in excess of \$30,000 during a calendar year. In light of recent national emergencies, the Section will lift this cap in order to give the Attorney General flexibility in determining whether to authorize overtime if necessary. The Department anticipates that the Attorney General will issue Departmental guidance regarding when it is appropriate to authorize overtime pay in an amount that would exceed the limitations that have been lifted.

Section 504 Secretary of State's Authority to Pay Rewards

This section amends section 36 of the State Department's Basic Authorities Act of 1956 to enhance the ability of the Department of State to pay rewards to assist in bringing terrorists to justice. The section would expand the bases for which the Department could authorize payment of terrorism rewards, eliminate the overall limitation on the amount of funds that can be appropriated to the Department to carry out the rewards program, and eliminate the requirement

that the Department distribute funds equally for the purpose of preventing acts of international terrorism and narcotics trafficking. This section also raises the amount the Department could offer and pay under the program from \$5M to \$10M and allows the Secretary to authorize payment of an award larger than \$10M if the Secretary determines that doing so would be important to the national security interests of the United States.

Section 505 Assistance to Countries Co-Operating Against International Terrorism

Subsection (a) of this provision would give important new extraordinary authority for five years to the President to provide assistance or take other beneficial actions in favor of countries that support US efforts to fight international terrorism. Subsection (b) would allow the President to provide anti-terrorism assistance to entities, as well as countries, without being subject to any restrictions. Subsection (c) allows the President to provide assistance for non-proliferation and export control activities without restrictions. Both (b) and (c) also include illustrative lists of the types of assistance that may be provided pursuant to this authority.