U.S. Department of Justice

Executive Office for United States Attorneys
Freedom of Information/Privacy Act Staff
600 E Street, N.W., Room 7300
Washington, D.C. 20530
202-616-6757 Fax 202-616-6478

JAN 1 1 2007

Requester: Marcia Hoffmann Request Number: 06-3203

Subject of Request: Pen Register Guidance

Dear Requester:

Your request for records under the Freedom of Information Act/Privacy Act has been processed. This letter constitutes a reply from the Executive Office for United States Attorneys, the official record-keeper for all records located in this office and the various United States Attorneys' Offices.

To provide you the greatest degree of access authorized by the Freedom of Information Act and the Privacy Act, we have considered your request in light of the provisions of both statutes.

The records you seek are located in a Privacy Act system of records that, in accordance with regulations promulgated by the Attorney General, is exempt from the access provisions of the Privacy Act. 28 CFR § 16.81. We have also processed your request under the Freedom of Information Act and are making all records required to be released, or considered appropriate for release as a matter of discretion, available to you. This letter is a [**X**] partial [ ] full denial.

Enclosed please find:

__58__ page(s) are being released in full (RIF);
_____ page(s) are being released in part (RIP);
_____ page(s) are withheld in full (WIF). **The redacted/withheld documents were reviewed to determine if any information could be segregated for release.**

The exemption(s) cited for withholding records or portions of records are marked below. An enclosure to this letter explains the exemptions in more detail.

Section 552			Section 552a
[ ] (b)(1)	[ ] (b)(4)	[ ] (b)(7)(B)	[**X**] (j)(2)
[ ] (b)(2)	[ ] (b)(5)	[ ] (b)(7)(C)	[ ] (k)(2)
[ ] (b)(3)	[ ] (b)(6)	[ ] (b)(7)(D)	[ ] (k)(5)
_____	[ ] (b)(7)(A)	[ ] (b)(7)(E)	[ ] _____
_____		[ ] (b)(7)(F)	

[ ] In addition, this office is withholding grand jury material which is retained in the District.

Form No. 021- no fee - 2/06

[ ] A review of the material revealed:

[X] 149 page(s) originated with another government component. **These records were found in the U.S. Attorney's Office files and may or may not be responsive to your request.** These records will be referred to the following component(s) listed for review and direct response to you: Office of Information & Privacy (120 Pages) & Criminal Division (29 Pages).

[ ] There are public records which may be obtained from the clerk of the court or this office, upon specific request. If you wish to obtain a copy of these records, you must submit a new request. These records will be provided to you subject to copying fees.

[ ] Please note that your original letter was split into separate files ("requests"), for processing purposes, based on the nature of what you sought. Each file was given a separate Request Number (listed below), for which you will receive a separate response:

[ ] See additional information attached.

This is the final action on this above-numbered request. You may appeal this decision on this request by writing within 60 days from the date of this letter to the **Office of Information and Privacy, United States Department of Justice, 1425 New York Avenue, Suite 11050, Washington, D.C. 20530-0001**. Both the letter and envelope should be marked "FOIA Appeal." If you are dissatisfied with the results of any such administrative appeal, judicial review may thereafter be available in U.S. District Court, 28 C.F.R. §16.9.

Sincerely,

William G. Stewart II
Acting Assistant Director

Enclosure(s)

Requester: **Marcia Hoffmann**
FOIA #: **06-3203**

Continuation Sheet:

Please note that your original letter have been split into four separate files ('requests"), for processing purposes, depending on the nature of what you sought. Each file will have a separate Request Number (listed below), for which you will receive a separate response: 06-3201, 06-3202, 06-3203, & 06-3204.

This response is to FOIA No. 06-3203 only and does not include search results associated with the other requests listed above.

EXPLANATION OF EXEMPTIONS

FOIA: TITLE 5, UNITED STATES CODE, SECTION 552

(b) (1) (A) specifically authorized under criteria established by and Executive order to be kept secret in the in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual.

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

PRIVACY ACT: TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information complied in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to Executive Order 12356 in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material complied for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability eligibility, or qualification for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his identity would be held in confidence.

REQUESTER: Maria Hoffmann

FOIA FILE#: 06-3203

DOCUMENTS Released in Full "RIF"

58 pages

Department of Justice

FOR IMMEDIATE RELEASE
FRIDAY, OCTOBER 26, 2001
WWW.USDOJ.GOV

AG
(202) 616-2777
TDD (202) 514-1888

ATTORNEY GENERAL ASHCROFT DIRECTS LAW ENFORCEMENT OFFICIALS TO IMPLEMENT NEW ANTI-TERRORISM ACT

WASHINGTON, D.C. – Attorney General John Ashcroft today directed all 94 U.S. Attorneys' offices and 56 FBI field offices to implement the new anti-terrorism legislation overwhelmingly passed by Congress and today signed by President Bush. The new offensive against terrorism will require law enforcement to make use of new powers in intelligence gathering, criminal procedure and immigration violations. With these enhanced provisions, the fight against terrorism will have the full force of the law while protecting Constitutional civil liberties.

"Law enforcement is now empowered with new tools and resources necessary to disrupt, weaken, and eliminate the infrastructure of terrorist organizations, to prevent or thwart terrorist attacks, and to punish the perpetrators of terrorist acts," said Ashcroft. "The American people can be assured law enforcement will use these new tools to protect our nation while upholding the sacred liberties expressed in the Constitution."

The new provisions have two over-arching principles: airtight surveillance of terrorists and speed in tracking down and intercepting terrorists. Law enforcement has had many of these provisions to fight drug trafficking and organized crime, but previously they did not apply for terrorism. The Department's objective of preventing terrorist acts before they happen is strengthened dramatically and, therefore, the war on terrorism is escalated to a degree commensurate with the threat posed by terrorism. The legislation enacted today provides these new weapons in the war on terrorism:

- Prosecutors will seek judicial authority to intercept communications related to an expanded list of terrorism-related crimes such as: the development, possession, or use of chemical or biological weapons; financial transaction with a terrorist government; or providing material support to terrorists or terrorist organizations. Investigators will use "roving" wiretaps to intercept communications and thereby thwart the ability of terrorists to evade surveillance by switching phones or communication devices.

- Investigators will now aggressively pursue terrorists on the Internet. The legislation permits investigators to obtain senders' and receivers' e-mail addresses just as it is done with telephone surveillance. Terrorists employ sophisticated technologies to evade detection and the legislation updates the law to the technology. Investigators will use search warrants to obtain unopened voice-mail and email.

- New subpoena power will enable authorities to obtain payment information, such

RIF

as credit card or bank account numbers, of suspected terrorists on the Internet. This will allow investigators to identify the terrorist who hides behind a fictitious Internet name.

- Investigators will be able to use a single court order to trace a communication nationwide, even when it travels beyond the judicial district that issued the order. The scope of search warrants for unopened e-mail and other evidence will also be nationwide. This improved efficiency will save hours or days in investigations where seconds matter.

- Law enforcement and intelligence communities will share information on terrorist activities and thus better coordinate their efforts to prevent terrorism.

These new tools for law enforcement are the products of hundreds of hours of consultation and careful consideration by the Administration, members of Congress, and state and local officials. They are careful, balanced, and long overdue improvements in law enforcement's capacity to prevent terrorism.

###

01-558

Final Bill
Section-by-Section Analysis

Bill Provision No.	Bill Description
1	Title and table of contents.
2	Construction and severability clause.
101	Establishes a fund to reimburse DOJ components for costs incurred to rebuild facilities, investigate and prosecute terrorism, and to reimburse other Federal agencies for detaining individuals in foreign countries accused of terrorist acts.
102	Sense of Congress condemning discrimination against Arab and Muslim Americans.
103	Authorizes $200M for each of FY 2002, 2003 and 2004 for the FBI Technical Support Center (established by AEDPA).
104	Broadens Attorney General's authority to request assistance of Secretary of Defense in emergency situations involving weapons of mass destruction.
105	Directs the Secret Service to develop a national network of electronic crime task forces modeled on the New York task force.
106	Grants President the power to confiscate and take title to enemies' property, when United States has been attacked or is engaged in military hostilities; also authorizes courts to consider classified evidence, without making it public, in lawsuits that challenge the government's seizure of property.
201	Adds terrorism statutes—including chemical weapons offenses under 18 U.S.C. 22—as predicate offenses for which Title III wiretap orders are available.
202	Allows voice wiretaps in computer hacking investigations.
203(a)	Permits sharing of grand jury information regarding foreign intelligence and counterintelligence with federal law-enforcement, intelligence, protective, immigration, national defense and national security personnel; must notify court that disclosure has taken place. Can share grand jury information with state officials upon court order.
203(b)	Sharing of wiretap information regarding foreign intelligence, counterintelligence, and foreign intelligence information with federal law-enforcement, intelligence, protective, immigration, national defense and national security personnel.
203(c)	Requires AG to establish procedure for information sharing in 203(a) and (b).
203(d)	Permits sharing of information regarding foreign intelligence, counterintelligence, and foreign intelligence information with federal law-enforcement, intelligence, protective, immigration, national defense and national security personnel notwithstanding other law.
204	Assures that foreign intelligence gathering authorities are not disrupted by changes to pen register/trap and trace statute.
205	Employment of translators by the FBI.

206	Allows court to authorize roving surveillance under FISA where court finds that the actions of the target may have effect of thwarting the identification of a target.
207	Initial authorization for surveillance and search of officers/employees of foreign powers changed to 120 days; can be extended for one year period. All other searches authorized for 90 day period.
208	Increases the number of judges on the FISA Court to 11, no less than 3 of whom must live within 20 miles of Washington, D.C.
209	Allows voice mail stored with a third party provider to be obtained with a search warrant, rather than a wiretap order.
210	Broadens the types of records that law enforcement can subpoena from communications providers, including the means and source of payment.
211	Clarifies that statutes governing telephone and internet communications (and not the burdensome provisions of the Cable Act) apply to cable companies that provide internet or telephone service in addition to television programming.
212	Allows computer-service providers to disclose communications and records of communications to protect life and limb; and clarifies that victims of computer hacking can disclose non-content records to protect their rights and property.
213	Amends 18 U.S.C. 3103a to permit delayed notice of search warrants where court determines that immediate notice would have an "adverse result"; officers may seize property if court finds "reasonable necessity."
214	To get pen register/trap and trace order under FISA, must certify that information likely to be obtained is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities; investigations of US persons may not be conducted upon the basis of First Amendment protected activities.
215	Business records provision allows any designee of FBI director no lower than Assistant Special Agent in Charge to apply to FISA court or a magistrate designated by Chief Justice for an ex parte order requiring production of any tangible things for an investigation to protect against international terrorism or clandestine intelligence activities; investigation must be conducted under AG Guidelines under EO 12333, and investigation of a US person cannot be based on First Amendment protected behavior; also requires semiannual reporting to Congress.
216	Amends the pen register/trap and trace statute to apply to internet communications, and to allow for a single order valid across the country.
217	Allows victims of computer-hacking crimes to request law enforcement assistance in monitoring trespassers on their computers; "computer trespasser" does not include persons who have a contractual relationship with the hacked computer's owner.
218	Allows law enforcement to conduct surveillance or searches under FISA if "a significant purpose" is foreign intelligence
219	Permits courts to issue search warrants that are valid nationwide for investigations involving terrorism.
220	Permits courts to issue search warrants for communications stored by providers anywhere in the country; court must have jurisdiction over the offense.
221	Authorizes President to impose sanctions relating to the export of devices that could be used to develop missiles or other weapons of mass destruction. Also expands President's ability to restrict exports to the portions of Afghanistan controlled by the Taliban.

222	Protects communications providers from having to develop or deploy new technology as a result of the Bill, and assures that they will be reasonably compensated.
223	Creates a cause of action and authorizes money damages against the United States if officers disclose sensitive information without authorization.
224	Provides that all changes in Title II sunset after four years (except sections 203(a), 203(c), 205, 208, 210, 211, 213, 216, 219, 221, and 222).
225	Grants immunity from civil liability to persons who furnish information in compliance with a FISA order.
301	Title of money-laundering act.
302	Congressional findings.
303	Sunset provision; money-laundering provisions will expire in 2005 if Congress enacts joint resolution.
311	Authorizes the Treasury Secretary to require that financial institutions undertake a variety of special measures to prevent money laundering, such as recording certain transactions and obtaining information about correspondent accounts.
312	Imposes special due diligence requirements for private banking and correspondent accounts that involve foreign persons.
313	Prohibits domestic financial institutions from maintaining correspondent accounts with foreign shell banks.
314	Requires Treasury Secretary to promulgate regulations to encourage cooperation among financial institutions, regulators, and law enforcement; allows financial institutions to share information regarding persons suspected of terrorism-related money laundering.
315	Includes various foreign-corruption offenses—including bribery and smuggling—as "specified unlawful activities" under the money-laundering statute.
316	Allows persons to contest confiscations of their property in connection with antiterrorism investigations.
317	Authorizes long-arm jurisdiction over foreign money launderers; also allows courts to restrain foreign-money launderers' assets before trial.
318	Essentially a technical amendment, defines "financial institution" to include a "foreign bank."
319	Permits forfeiture of funds held in United States interbank accounts; upon the request of federal banking agencies, requires financial institutions to disclose information about anti-money laundering compliance.
320	Authorizes the civil forfeiture of property related to certain offenses against foreign nations, including controlled-substances crimes, murder, and destruction of property.
321	Includes various entities in the definition of "financial institution,", including futures commission merchants and the Commodity Futures Trading Commission.
322	Provides that a statute preventing fugitives from using court resources in forfeiture actions, also applies to claims brought by corporations whose officers are fugitives. **[typo in bill; refers to title 18; should be title 28]**
323	Allows courts to issue restraining orders to preserve the availability of property subject to forfeiture by a foreign government.

324	Requires Treasury Secretary to report on the operation of this subtitle.
325	Allows Treasury Secretary to issue regulations governing concentration accounts, to ensure that customers cannot secretly move funds.
326	Requires Treasury Secretary to promulgate rules requiring financial institutions to verify the identities of persons opening accounts.
327	Requires the government to consider financial institutions' anti-money laundering record when deciding to approve various requests, including proposed mergers.
328	Requires Treasury Secretary to cooperate with foreign governments to identify the originators of wire transfers.
329	Imposes criminal penalties on government employees who is bribed in connection with his duties under the money-laundering title.
330	Sense of Congress that the United States should negotiate with foreign nations to secure their cooperation in investigations of terrorist groups' finances.
351	Grants immunity to a financial institution that voluntarily discloses suspicious transactions; prohibits the institution from notifying the person who conducted the suspicious transaction that it has been reported.
352	Directs financial institutions to establish anti-money laundering programs, and allows Treasury Secretary to prescribe minimum standards.
353	Imposes civil and criminal penalties for violations of geographic targeting orders; extends the effective period for geographic targeting orders from 60 to 180 days.
354	Requires the President's national strategy on money laundering to include data regarding the funding of international terrorism.
355	Allows financial institutions to disclose suspicious activity in employment references.
356	Obliges Treasury Secretary to issue regulations that require securities brokers and commodities merchants to report suspicious activities.
357	Requires Treasury Secretary to report on the administration of Bank Secrecy Act provisions.
358	Makes various amendments to Bank Secrecy Act to enhance United States's ability to fight international terrorism, including making information available to intelligence agencies.
359	Requires reporting on the suspicious activities of underground banking systems.
360	Instructs United States Executive Directors of international financial institutions to use their voice and vote to support loans to foreign countries that assist the United States' fight against international terrorism.
361	Establishes procedures and rules governing the Treasury Department's Financial Crimes Enforcement Network.
362	Requires Treasury Secretary to establish in the Financial Crimes Enforcement Network, a highly secure network that will allow the exchange of information with financial institutions.
363	Increases civil and criminal penalties for money laundering.
364	Authorizes the Federal Reserve to hire security personnel.

365	Requires companies that receive more than $10,000 in currency in a transaction to file a report with the Financial Crimes Enforcement Network.
366	Requires Treasury Secretary to study expanding exemptions from currency reporting requirements.
371	Makes it a crime to smuggle more than $10,000 in currency into or out of the United States, with the intent of avoiding a currency reporting requirement; also authorizes civil forfeiture.
372	Authorizes criminal and civil forfeiture in currency-reporting cases.
373	Includes a scienter requirement for the crime of operating an unlicenced money transmitting business.
374	Increases penalties for counterfeiting United States currency and obligations; clarifies that counterfeiting statutes apply to counterfeits produced by electronic means.
375	Increases penalties for counterfeiting foreign currency and obligations.
376	Designates a new predicate money-laundering offense: providing material support or resources to foreign terrorist organizations in violation of 18 U.S.C. § 2339B.
377	Provides for extraterritorial jurisdiction over certain crimes of fraud in connection with access devices.
401	Authorizes AG to waive caps on immigration personnel assigned to protect Northern Border
402	Triples the number of Border Patrol personnel, Customs Service personnel, and Immigration and Naturalization Service inspectors; also allocates an additional $50 million each to the Customs Service and the INS.
403	Requires the FBI to share criminal-record information with the INS and the State Department for the purpose of adjudicating visa applications.
404	One-time expansion of INS authority to pay overtime
405	Requires AG to report to Congress on feasibility of enhancing FBI's Integrated Automated Fingerprint Identification System, or "IAFIS," to prevent foreign terrorists from receiving visas and from entering United States
411	Broadens the Immigration and Nationality Act's terrorism-related definitions. Expands grounds of inadmissibility to include persons who publicly endorse terrorist activity. Expands definition of "terrorist activity" to include all dangerous devices in addition to firearms and explosives. Expands definition of "engaging in a terrorist activity" to include providing material support to groups that the person knows or should know that are terrorist organizations, regardless of whether the support's purpose is terrorism related.
412	Requires AG to detain aliens whom he certifies as threats to national security. AG must charge aliens with criminal or immigration offenses within seven days. AG must detain aliens until they are removed or until he determines that they no longer pose threat. Establishes D.C. Circuit as exclusive jurisdiction for appeals
413	Gives Secretary of State discretion to provide visa-records information to foreign governments, for the purpose of combating international terrorism or crime; gives certain countries general access to State Department's lookout databases
414	Sense of Congress regarding need to expedite implementation of an integrated entry and exit data system.

415	Provides that Office of Homeland Security shall participate in the entry-exit task force authorized by Congress in 1996.
416	Requires AG to implement fully and expand the foreign student visa monitoring program authorized by Congress in 1996.
417	Requires Secretary of State to enhance efforts to develop machine-readable passports.
418	Obliges Secretary of State to review how consular officers issue visas to determine whether consular shopping is a problem.
421	Grants special immigrant status to people who were in the process of securing permanent residence through a family member who died, was disabled, or lost employment as a result of the September 11 attacks.
422	Provides a temporary extension of status to people who are present in the United States on a "derivative status" (the spouse or minor child) of a non-immigrant who was killed or injured on September 11.
423	Provides that aliens whose spouses or parents were killed in the September 11 attacks will continue to be considered "immediate relatives" entitled to remain in the United States.
424	Provides that aliens who turn 21 during or after September 2001 shall be considered children for 90 or 45 days, respectively, after their birthdays
425	Authorizes AG to provide temporary administrative relief, for humanitarian purposes, to any alien who is related to a person killed by terrorists.
426	Requires AG to establish evidentiary guidelines for demonstrating that death or disability occurred as a result of terrorist activity.
427	Provides that no benefits shall be given to terrorists or their family members.
428	Definitions.
501	Enhances the AG's authority to pay rewards in connection with terrorism.
502	Enhances Secretary of State's authority to pay rewards in connection with terrorism.
503	Expands DNA sample collection predicates for federal offenders to include all offenses in 18 U.S.C. 2332b(g)(5)(B) list, all crimes of violence (as defined in 18 U.S.C. 16), and attempts and conspiracies to commit such crimes.
504	Allows "federal officers" who conduct FISA surveillance or searches to coordinate efforts to investigate or protect against attacks, grave hostile acts, sabotage, international terrorism, or clandestine intelligence activities by foreign power.
505	Allows FBI Deputy Assistant Director or higher (or Special Agent in Charge) to issue National Security Letters for telephone toll and transaction records, financial records, and consumer reports.
506	Extends Secret Service's jurisdiction (concurrently with FBI's) to investigate offenses against government computers.

507	Person not lower than Assistant AG can apply for an ex parte court order to obtain educational records that are relevant to an authorized investigation or prosecution of a grave felony or an act of domestic or international terrorism; must provide specific and articulable facts showing that records likely to contain information related to the offenses; AG required to issue guidelines to protect confidentiality.
508	Eliminates restrictions on production of information from National Center for Education Statistics; allows person not lower than Assistant AG to collect information if there are specific and articulable facts that records are likely to contain information related to a grave felony or an act of domestic or international terrorism; AG required to issue guidelines to protect confidentiality.
611	Provides for expedited payment of Public Safety Officer benefits in connection with terrorism.
612	Technical amendments to Pub. L. 107-37.
613	Raises base amount of Public Safety Officer benefits from $100K to $250K.
614	Enhances authority of Assistant Attorney General for the Office of Justice Programs to manage OJP.
621	Makes many minor changes in crime victims compensation program; one is: amounts received by the Crime Victims Fund from the $40B emergency fund are not subject to spending cap.
622	Makes many minor changes in the crime victims compensation program.
623	Makes many minor changes in the crime victims compensation program.
624	Makes many minor changes in the crime victims compensation program; one expands use of its emergency reserve.
701	Expands regional information-sharing system to enhance federal and state law-enforcement officers' ability to respond to terrorist attacks.
801	Makes it a crime to engage in terrorist attacks on mass transportation systems.
802	Adds definition of "domestic terrorism" to 18 U.S.C. 2331 and makes conforming change in existing definition of "international terrorism."
803	Makes it a crime to harbor a person where perpetrator knows or has reasonable grounds to believe that the person has committed or is about to commit one of several serious terrorism crimes; includes venue provision.
804	Extends the United States' special maritime and territorial jurisdiction to any offenses committed by or against U.S. nationals at foreign missions and related residences; excludes offenses by persons covered under 18 U.S.C. 3261(a) (which provides separate extraterritorial provision for persons accompanying the armed forces).
805	Amends crime of providing material support to terrorists by deleting the "within the U.S." restriction; adds some additional predicate offenses; and adds "monetary instruments" and "expert advice or assistance" as types of prohibited support. Also, adds material support of foreign terrorist organizations as money laundering predicate.
806	Amends 18 U.S.C. 981(a)(1) to authorize civil forfeiture of all assets owned by persons engaged in terrorism.
807	Clarifies that Trade Sanctions Reform and Export Enhancement Act of 2000 does not limit the prohibition on providing material support to terrorists or foreign terrorist organizations.

808	Amends definition of "federal crime of terrorism" in 18 U.S.C. 2332b(g)(5)(B) to include a number of serious crimes that terrorists are likely to commit. Makes conforming amendment to 2332b(f) to avoid reducing AG's primary investigative jurisdiction;
809	No statute of limitations for certain terrorism crimes that involve the occurrence or foreseeable risk of death or serious injury; other terrorism crimes subject to extended eight-year limitations period.
810	Amends statutes defining various terrorism crimes (including arson and material support to terrorists) to provide base maximum prison terms of 15 or 20 years, and up to life imprisonment where death results.
811	Amends statutes defining various terrorism crimes (including arson and killings in federal facilities) to add a prohibition on attempt and conspiracy; provides increased penalties for attempts and conspiracies that are equal to the penalties for the underlying offenses.
812	Authorizes postrelease supervision periods of up to life for persons convicted of terrorism crimes that involved the occurrence or foreseeable risk of death or serious injury.
813	Adds terrorism crimes listed in 18 U.S.C. 2332b(g)(5)(B) as predicates under RICO.
814	Makes a number of amendments to the computer hacking law to clarify protection of protected computers, and to ensure adequate penalties for cyber-terrorists.
815	Creates a defense for persons who disclose wire or electronic communications records in response to the request of a governmental entity.
816	Requires AG to establish regional computer forensic laboratories to enhance cybersecurity.
817	Broadens prohibition on possessing biological toxins: unlawful to possess toxins for anything other than a peaceful purpose; makes it a crime to possess a biological toxin in a quantity suggesting defendant had no peaceful purpose; provides that a small category of restricted persons (felons, illegal aliens and others) are disqualified from possessing biological toxins.
901	Gives CIA Director responsibility to establish requirements and priorities for foreign intelligence information under FISA, and to assist AG in ensuring that information derived from FISA surveillance or searches is used effectively for foreign intelligence purposes.
902	Includes international terrorist activities within the scope of foreign intelligence under the National Security Act.
903	Sense of Congress on the need to establish intelligence relationships to acquire information on terrorists.
904	Grants CIA Director temporary authority to delay submitting reports to Congress on intelligence matters.
905	Requires AG to disclose to CIA Director any foreign intelligence acquired by a DOJ element during a criminal investigation; AG can provide exceptions for classes of information to protect ongoing investigations.
906	Requires AG, CIA Director, and Secretary of the Treasury to report to Congress on feasibility of developing capacity to analyze foreign intelligence relating to terrorist organizations' finances.
907	Obliges Directors of FBI and CIA to report on the development of a "National Virtual Translation Center," which will provide intelligence community with translations of foreign intelligence

908	Requires AG to establish a program to train government officials in the identification and use of foreign intelligence.
1001	Directs DOJ Inspector General to review allegations that DOJ employees engaged in civil rights abuses.
1002	Sense of Congress that Sikhs should not be subject to discrimination in retaliation for the September 11 attacks.
1003	Defines "electronic surveillance" in FISA to exclude the acquisition of computer trespassers' communications.
1004	Provides that money laundering prosecutions may be brought in any district where the transaction occurred, or in any district the underlying unlawful activity could be prosecuted.
1005	Requires AG to make grants to enhance states and local governments' ability to respond to and prevent terrorism.
1006	Provides that aliens who are engaged in money laundering may not be admitted to the United States.
1007	Authorizes Drug Enforcement Administration funds for antidrug training in Turkey and in South and Central Asia.
1008	Requires AG to study feasibility of using fingerprint scanner at overseas consular posts and points of entry into the United States.
1009	Requires FBI to report to Congress on feasibility of providing airlines with names of passengers who are suspected to be terrorists.
1010	Allows Defense Department to contract with state and local governments to provide security at military installations during Operation Enduring Freedom.
1011	Enhances statutes making it unlawful to fraudulently solicit charitable contributions.
1012	Restricts states' ability to issue licenses to transport hazardous materials; Transportation Secretary must first determine that licensee poses no security risk.
1013	Sense of the Senate that the United States should increase funding for bioterrorism preparedness.
1014	Requires Office of Justice Programs to make grants to states to enhance their ability to prepare for and respond to terrorism involving weapons of mass destruction.
1015	Expands and reauthorizes the Crime Identification Technology Act for antiterrorism grants to states and localities.
1016	Establishes National Infrastructure Simulation and Analysis Center to protect United States' critical infrastructure from terrorist attacks.

USA PATRIOT Act of 2001
Overview and Talking Points

Overview

In the wake of the tragic, criminal act of violence perpetrated against the United States on September 11, the Bush Administration proposed legislation that would provide the Department of Justice with the tools and resources necessary to disrupt, weaken, and counter the infrastructure of terrorist organizations, to prevent or thwart terrorist attacks, and to punish or defeat in battle perpetrators of terrorist acts.

On October 24, the House passed a bill which contains a substantial number of the key provisions originally requested by the Administration. The Department of Justice strongly supports this bill and urges the Senate to act quickly so that these new authorities can be made available to prosecutors and agents who are working around the clock to prevent future attacks and to bring the perpetrators of September 11 to justice.

The events of September 11, 2001 demonstrate that terrorist acts are perpetrated by expertly organized, highly coordinated, and well financed organizations, operating without regard to borders, to advance their agendas. The fight against terrorism thus is both a war to defend the security of our nation and our citizens against terrorism and a unified criminal justice effort.

Existing laws fail to provide our national security authorities and law enforcement with certain critical tools they need to fight and win the war against terrorism. Indeed, we have tougher laws for fighting organized crime and drug trafficking than for combating the threat of terrorism. For example, technology has dramatically outpaced our statutes. Many of our most important intelligence gathering laws were enacted decades ago, in and for an era of rotary telephones. Meanwhile, our enemies use email, the Internet, mobile communications and voice mail. Until Congress provides law enforcement with the tools necessary to identify, dismantle and punish terrorist organizations, we are fighting an uphill battle.

Making the fight against terrorism a national priority must not and will not mean that the rights and freedoms guaranteed to all Americans under the Constitution will become victims of this war. In this law enforcement mission, as in all that we undertake at the Department of Justice, the protection of the rights and privacy of all Americans is the principle that guides us – the outcome which, if not achieved, renders our efforts meaningless.

This new terrorist threat to Americans on our soil is a turning point in America's history. It is a new challenge for law enforcement. Our fight against terrorism is not solely or primarily a criminal justice endeavor -- it is defense of our nation and its citizens. We cannot wait for terrorists to strike to begin investigations and take action. We must prevent first, and prosecute second. The anti-terrorism proposals that have been submitted by the Administration and considered by the House and Senate represent careful, balanced, and long overdue improvements

to our capacity to combat terrorism.

STATUS OF LEGISLATION

- The Administration reached bipartisan agreement with the leadership of the House and Senate and the chairmen and ranking members of the Senate and House Judiciary Committees on a bill which was passed by the House on October 24 by an overwhelming majority.

- The Department of Justice strongly supports this bill and urges the Senate to act quickly so that these new authorities can be made available to prosecutors and agents who are working around the clock to prevent future attacks and to bring the perpetrators of September 11 to justice. Although the compromises reflected in specific provisions of the bill do not in every case meet the Administration's original goals, the bill does overall substantially achieve each and every one of the Administration's objectives.

TALKING POINTS ON SUBSTANTIVE PROVISIONS

Enhancing Domestic Security Against Terrorism (Title I)

- These provisions would provide new funding and structural reforms in the fight against terrorism. A counterterrorism fund would be established to address terrorism issues within the Department of Justice with regard to investigations and damage to components as a result of terrorism (§ 101); discrimination against Arab and Muslim Americans is condemned (§ 102); additional funding would be provided for the FBI's technical support center (§ 103); the National Electronic Crime Task Force Initiative would be expanded (§ 105); and the military would be authorized to assist state and local law enforcement in chemical weapons emergencies (§ 104).

- The President's powers under the International Economic Emergency Powers Act would be expanded in cases of military hostilities and regarding the use of classified information (§ 106). President Bush signed a new Executive Order under the International Emergency Economic Powers Act (IEEPA) blocking the assets of, and transactions with, terrorist organizations and certain charitable, humanitarian, and business organizations that finance or support terrorism. At present, however, the President's powers are limited to freezing assets and blocking transactions with such individuals and entities. Starving terrorist organizations of the funds that sustain them requires that we do more. When we encounter drug traffickers, for instance, we don't just freeze assets, we seize assets.

Enhanced Surveillance Procedures (Title II)

- These provisions of the bill address gaps in the coverage of the federal electronic surveillance statutes (particularly the wiretap statute, the pen registers and trap and trace statute, and the Electronic Communications Privacy Act). The key element that unites

these provisions is the goal of making the statutes technology-neutral: that is, ensuring that the same existing authorities that apply to telephones, for example, are made applicable to computers and use of e-mail on the Internet. It is critically important to note that in drafting these provisions, the Department's goal was and remains ensuring that the scope of the authority remains the same -- in other words, that no more or less information as is currently obtainable through a particular device (for example, a pen register) on a telephone, is obtainable from a computer.

- Law enforcement must have intelligence gathering tools that match the pace and sophistication of the technology utilized by terrorists. Critically, we also need the authority for law enforcement to share vital information with our national security and intelligence agencies in order to prevent future terrorist attacks.

- Terrorist organizations increasingly take advantage of technology to hide their communications from law enforcement. Today's terrorist communications are carried over multiple mobile phones and computer networks – frequently by multiple telecommunications providers located in different jurisdictions. To facilitate their criminal acts, terrorists do not discriminate among different kinds of technology. Regrettably, our intelligence gathering laws don't give law enforcement the same flexibility.

- The bill creates a technology-neutral standard for intelligence gathering, ensuring law enforcement's ability to trace the communications of terrorists over mobile phones, computer networks and any new technology that may be developed in the coming years.

- We are not seeking changes in the protections in the law for the privacy of law-abiding citizens. The bill would streamline intelligence gathering procedures only. Except for under those circumstances authorized by current law, the content of communications would remain off-limits to monitoring. The information captured by this technology-neutral standard would be limited to the kind of information you might find in a phone bill, such as the phone numbers dialed by a particular telephone.

- The Department strongly opposed the two-year "sunset" on these critical provisions in the original House version of the legislation. The President and the Attorney General have stressed that the threat of terrorism will not "sunset;" rather the fight against terrorism will be a long struggle, and law enforcement must have the necessary tools to fight this war over the long term. However, law enforcement must have these tools now. To calm fears of a permanent authority, the bill now includes a four year "sunset" provision for several provisions as noted during the discussion of the impacted provisions, at which time it is the Administration's hope that these changes in surveillance law will be made permanent.

Foreign Intelligence Surveillance Act (FISA) Amendments (Title II)

- These provisions sharpen the tools used by the FBI, CIA, and NSA for collecting intelligence on international terrorists and other targets under FISA, 50 U.S.C. §§ 1801-63. The amendments in this area would enable the agents and case officers of the FBI and CIA and the analysts of NSA to respond more quickly and efficiently to crises and to operational opportunities against terrorists and other targets.

Period of FISA Surveillance and Search Orders

- Problem: Currently, with limited exceptions, applications to the FISA Court for its authorization to conduct electronic surveillance and physical search must be renewed by the Court every 90 and 45 days, respectively. Applications to the Court for surveillance and search against foreign terrorists and spies are noncontroversial but bog down the agencies and clog the Court.

- Solution: The legislation would, for the conduct of electronic surveillance and physical search against foreign terrorists and spies, extend the duration of an approval order to 120-days with extension possible for up to a year for electronic surveillance and would extend the duration for searches from 45 to 90 days. (§ 207). This provision would sunset in four-years.

Multi-Point Authority

- Problem: Foreign terrorists and spies are trained to change mobile or ground-line phones, hotel rooms, and restaurants in order to defeat surveillance. Currently, to effect FISA coverage at a new facility, DOJ must develop and draft a new application, get it certified by the Director of FBI and signed by the Attorney General, and find and present it to a judge on the FISA Court. This delays or defeats our coverage of these targets and impairs our ability to investigate and detect terrorism and espionage.

- Solution: The bill would enable the FBI, in response to such actions by FISA targets that thwart coverage (§ 206), to serve an order on a previously unidentified vendor or facility in order to maintain the coverage. Congress passed a similar provision for Title III a few years ago. These provisions will sunset in four years.

Mobility - Nationwide Search Warrants

- As communications technology now provides significant mobility to its users, who can pass from jurisdiction to jurisdiction in minutes, law enforcement and intelligence officers need that same flexibility.

- The bill provides for nationwide search warrants for voice mail (§ 209), e-mail (as long as the issuing court has jurisdiction over the offense being investigated) (§ 220), and in investigations involving terrorism (§ 219).

Foreign Intelligence Information

- Problem: Currently, as interpreted, the FISA requires that the FBI Director or other senior official certify that the collection of foreign intelligence is "the purpose" of the FISA search or surveillance. As interpreted by the FISA Court, that standard has hindered the Department's ability to coordinate multi-faceted responses to international terrorism, which involve foreign intelligence and criminal investigations and equities.

- Solution: The bill would change this standard. The bill would require certification that the collection of foreign intelligence is "a significant purpose," rather than "the purpose," of the FISA search or surveillance; however, this provision is subject to the four-year sunset applicable to several FISA provisions. (§ 218).

Foreign Intelligence Information Sharing

- Problem: Currently, with few exceptions, criminal investigators may not share grand jury or Title III information with the intelligence agencies. Records obtained through grand jury subpoenas and insights gained through Title III remain inaccessible to agencies that need such information in their operations and analysis.

- Solution: The bill would enable foreign intelligence information obtained in a criminal investigation, including information obtained through a grand jury or Title III, to be shared with intelligence and other federal officers, subject to the four-year sunset and would require the court to be notified after any such information sharing occurs in the case of grand jury information. (§ 203). In addition, the Attorney General must establish procedures for the release of information when it pertains to a case against a United States citizen. Also, the FBI has been authorized to expedite the hiring of translators capable of translating any information gathered under these and other procedures (§ 205).

Pen Register; Business Records; National Security Letters

- Problem: The ability of the FBI to obtain basic records as a part of an international terrorist or other intelligence investigation has been hampered by cumbersome procedures concerning pen registers, business records, and national security letters. As the current investigation of flight school records makes clear, our ability to gain quick access to such information may be critical to an investigation.

- Solution: The legislation would enable the FBI to obtain toll, business, and other records more efficiently by eliminating the requirement of a showing that there is a nexus to a foreign power, and applying a standard of relevance to an intelligence or counterintelligence investigation. This new standard is limited to protection against international terrorism or clandestine intelligence activities and may not be based solely on First Amendment activities. (§§ 214, 215, 216). Pen/trap provisions would also now apply to Internet traffic, as well as telephone communications, while excluding Internet

Service Providers (ISPs) and other entities complying with wiretap orders from liability based on any surveillance under these provisions. (See also §§ 201, 202, expanding predicates for obtaining surveillance authority). These provisions are subject to the four-year sunset.

Broadened Scope of Subpoenas for Records of Electronic Communications and Subscriber Records

- The bill would permits the disclosure of information such as means of payment for electronic services, including bank account and credit card numbers, pursuant to subpoena. The bill would treat cable companies acting in their capacity of providing Internet services the same as other ISPs and telephone companies in this regard, removing them from the protections of laws governing cable privacy, the intent of which was and is to prevent disclosure of shows watched in the privacy of one's home not benign information such as account numbers and forms of payment. (§ 225). ISPs would also be permitted under the bill to disclose information of stored electronic communications where such communications indicate a risk of immediate death or injury. (§§ 210, 211, 212).

Delayed Notice of Execution of Search Warrant

- The bill would permit delayed notice of execution of a search warrant in criminal investigations, for a reasonable time thereafter, where notice of the execution would have an adverse result. (§ 213).

International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 (Title III)

- Title III of the bill is designed to impede the financing of terrorist activities. It accomplishes that goal by allowing the government to confiscate the assets of foreign terrorist organizations, the terrorists themselves and those who aid them. In addition, it allows the United States government to restrain those assets after indictment but before any final adjudication to ensure those assets are available to satisfy a judgment of forfeiture.

- Law enforcement must be able to "follow the money" in order to identify and neutralize terrorist networks.

- The bill gives law enforcement the ability to seize the assets of terrorist organizations. In addition, criminal liability is imposed on those who knowingly engage in financial transactions – money laundering – involving the proceeds of terrorist acts. In addition, financial institutions are encouraged to participate in this endeavor by providing civil liability immunity to financial institutions that disclose suspicious activity. (§ 314). The bill further includes financial institutions in this endeavor by requiring them to have

anti-money laundering programs. (§§ 314, 352).

- The bill would expand the scope of predicate money laundering offenses to include providing material support for terrorist organizations. (§ 301). These offenses would further not be limited to conduct occurring within the United States, as long as the tools of the offense are in or passed through the United States. (§§ 302, 377).

- Various common banking problems are also addressed in the bill, such as shell banks, correspondent accounts, and concentration accounts. (§§ 312, 313, 325). Treasury would be authorized to order special measures be taken by financial institutions where they are involved in such accounts or other primary money laundering concerns. (§ 311). Information would be made available as to such crucial facts as the beneficial, as opposed to nominal, owner of a bank account and minimum standards and policies would be put into effect to deal with correspondent and concentration accounts involving foreign persons. (§§ 312, 313, 325, 326).

- Employee references would be permitted to include reference to suspicious activity by the employee without fear of liability and other cooperation among financial institutions, law enforcement, and regulatory authorities would be encouraged. (§§ 314, 330, 355).

These money laundering provisions are all subject to the four-year sunset.

Protecting the Border (Title IV)

- The legislation expands the grounds for deeming an alien inadmissible or deportable from the United States for terrorist activity, provides for the mandatory detention of aliens whom the Attorney General certifies pose a risk to the national security, and facilitates information sharing within the U.S. and with foreign governments. Current law allows some aliens who are threats to the national security to enter and remain in the United States. The provisions in the bill correct those inadequacies and are necessary tools to prevent detain and remove aliens who are national security threats from the United States. The Attorney General would also have the authority to detain suspected terrorists who are threats to national security, as long as removal proceedings or criminal charges are filed within 7-days. (§ 412). In the rare cases where removal is determined appropriate but is not possible, detention may continue upon a review by the Attorney General every 6 months. (§ 412). The bill further would expand the definition of terrorists for purpose of inadmissibility or removal to include public endorsement of terrorist activity or provision of material support to terrorist organizations. (§ 411). The bill further expands the types of weapons the use of which can be considered terrorist activity. (§ 411).

- The ability of alien terrorists to move freely across borders and operate within the United States is critical to their capacity to inflict damage on the citizens and facilities in the United States. Under current law, the existing grounds for removal of aliens for terrorism are limited to direct material support of an individual terrorist. The bill would expand

these grounds for removal to include material support to terrorist organizations. (§ 412).

- To address the need for better border patrol, additional border patrol officers would be authorized, specifically on the northern border which has, during the investigation into the September 11th events, been shown to be extremely problematic. (§§ 401, 402). To aid INS agents, the FBI would also be required to provide criminal records information to those agents. (§ 403).

- The bill addresses not only unwelcome suspected terrorist aliens but also immigrants who may need additional consideration to stay within the United States where their loved ones were victims of terrorist activity. (§§ 421-428).

Removing Obstacles to Investigating Terrorism (Title V)

- The bill authorizes the Attorney General and Secretary of State to pay rewards related to terrorism investigations. It also provides for the DNA data collection from those convicted of terrorism offenses and the coordination of Federal law enforcement agencies. (§§ 501, 502, 503, 504).

Providing for Victims and Public Safety Officers (Title VI)

- The bill establishes procedures for expedited payment of public safety officers involved in the prevention, investigation, rescue or recovery efforts related to a terrorist attack, as well as providing increases to the Public Safety Officer Benefit Program. (§§ 611-614).

Increased Information Sharing (Title VII)

- The bill would require information sharing among Federal, State and Local law enforcement, thus, providing the necessary full picture needed to address terrorism. (§ 711).

Substantive Criminal Law/Criminal Procedure: Strengthening the Criminal Law Against Terrorism (Title VIII)

- These provisions reform substantive and procedural criminal law to strengthen federal law enforcement's ability to investigate, prosecute, prevent, and punish terrorist crimes. There are substantial deficits in each of these areas which impede or weaken our antiterrorism efforts.

- We must make fighting terrorism a national priority in our criminal justice system. Current law makes it easier to prosecute members of organized crime than to crack down on terrorists who can kill thousands of Americans in a single day. The same is true of

drug traffickers and individuals involved in espionage – our laws treat these criminals and those who aid and abet them more severely than terrorists.

- Our investigation has found that wide terrorist networks, not isolated individuals, are responsible for the September 11 attacks. Whether the members of these networks are in the United States or in other countries, they and those who aid them must be subject to the full force of our laws. Just as the law currently regards those who harbor persons engaged in espionage, the bill would make the harboring of terrorists a criminal offense. The bill also increases the penalties for conspiracy to commit terrorist acts to a serious level as we have done for many drug crimes.

Key Provisions

- Removing impediments to effective prosecution – elimination of statute of limitations for offenses creating the risk of death or personal injury and extending the statute for all other terrorism offenses to 8-years. (§ 809).

- Removing impediments to effective investigation – single jurisdiction search warrants; expanded jurisdiction to include terrorism against U.S. facilities abroad. (§ 804).

- Strengthening substantive criminal law – prohibition on harboring terrorists and on material support of terrorists (§§ 803, 805, 807); making terrorist crimes RICO predicates (§ 813); extending powers of asset forfeiture to terrorists' assets (§ 806); including altering cyberterrorism offense (§ 814); expanding the offense of possession of bioweapons (prohibiting possession of biological toxins by felons and aliens) (§ 817); creating a federal offense for attacking mass transportation systems (§ 801); expanding definition of domestic terrorism and offenses of the crime of terrorism, requiring a showing of coercion of government as an element of the offense (§§ 802, 808).

- Strengthening criminal penalties – longer prison terms and postrelease supervision of terrorists (§ 812); higher conspiracy penalties for terrorists (§ 811); alternative maximum sentences up to life for terrorism offenses (§ 810).

Improved Intelligence (Title IX)

- The bill authorizes the Director of the CIA to establish requirements and provide for the collection of foreign intelligence. The Director would also be asked to ensure proper dissemination of foreign intelligence information. Only if the appropriate officials have all the relevant information will prevention, investigation, and prosecution be fully functioning. The bill also would provide for the tracking of terrorist assets as part of the collection of information. (§§ 901, 905).

Miscellaneous (Title X)

The bill would finally require the Department of Justice Inspector General to designate an official to receive civil liberty and civil rights complaints and report those complaints to Congress. The presumption is that such information will be used in determining the continuing viability of the provisions in the bill subject to sunset in 2005. (§ 1001).

RUN DATE: 26-OCT-01 EXECUTIVE OFFICE OF UNITED STATES ATTORNEYS
CONTROL SHEET PAGE: 1

OPERATOR: KHUGHES

Control #: 200103917 EXESEC #:

FROM: ASHCROFT,JOHN
District:

Corresp. Date:	Received Date:	Due Date:
03-OCT-2001	05-OCT-2001	24-OCT-2002

Subject: SUPPORT OF THE PRESIDENT'S ORDER TO CALL UP THE RESERVE & GUARD

Remarks: ON SEPTEMBER 14, 2001, THE PRESIDENT SIGNED EXECUTIVE ORDER 13222 COPY ATTACHED ORDERING THE READY RESERVE OF THE ARMED FORCES TO ACTIVE DUTY FOR A PERIOD OF NOT MORE THAT 24 MONTHS TO RESPOND TO THE CONTINUING AND IMMEDIATE THREAT OF FURTHER ATTACKS ON THE UNITED STATES.

Signature: DIR Action Office: PRS

Assigned To:	Date:
DEFALAISE	05-OCT-2001
SCHWARTZ	09-OCT-2001
THERESA	24-OCT-2001

Status: CC: FO, LC;EIB PER LOU TRANSFER TO PRS FOR RESPONSE;EIB

File In:

Completion Date:

FYI - Below please find the following three materials relating to the Attorney General's testimony before the Senate Judiciary Committee today: a press release discussing the Attorney General's testimony and detailing information regarding the Department's use of Sec. 215 (in text); the Attorney General's prepared testimony (in text); and the letter to Congress providing detailed information about the Department's use of Sec. 213 (attached in PDF). We look forward to speaking to you this afternoon.

213 Letter (Specter).pdf

****

FOR IMMEDIATE RELEASE — AG
TUESDAY, APRIL 5, 2005 — (202) 514-2008
WWW.USDOJ.GOV — TDD (202) 514-1888

ATTORNEY GENERAL ALBERTO R. GONZALES CALLS ON CONGRESS TO RENEW VITAL PROVISIONS OF THE USA PATRIOT ACT

WASHINGTON, D.C. - Attorney General Alberto R. Gonzales today called for Congress to renew all 16 provisions of the USA PATRIOT Act that are scheduled to sunset at the end of 2005 and presented the Senate Judiciary Committee with new information regarding the Justice Department's use of certain PATRIOT Act provisions.

"The USA PATRIOT Act has been an integral part of the federal government's successful prosecution of the war against terrorism, and now is not the time to relinquish some of our most effective tools in the fight," said Attorney General Gonzales. "I look forward to working with members of the committee on a bipartisan basis to protect the security of the American people, and I am open to suggestions for clarifying and strengthening the Act. But let me be clear about one thing: I will not support any proposal that would undermine our ability to combat terrorism effectively."

The PATRIOT Act was passed by Congress with overwhelming bipartisan support following the terrorist attacks of September 11, 2001, and it has been instrumental in assisting law enforcement to dismantle terrorist cells, disrupt terrorist plots, and capture terrorists before they have been able to strike. Several of the Act's most important provisions are scheduled to expire on December 31, 2005, including sections 215 and 206.

Section 215 allows national security investigators to seek a court order requesting the production of relevant business records and other items, which grand juries frequently obtain in ordinary criminal investigations. This way, if a spy or international terrorism suspect were to be picked up by someone using a rental car, investigators can request a court order for car rental records or other tangible things that would help identify whomever he meets and move the investigation forward.

Each and every request for business records under section 215 must be approved in

advance by a federal judge. The Justice Department has stated previously that only records relevant to a national security investigation may be requested, and that the recipient of a court order under section 215 may both consult with an attorney and challenge the order in court. In his statement today, Attorney General Gonzales said that the Department would support technical modifications to section 215 that clarify those three points in the law.

In presenting new information recently declassified by the Justice Department to the committee, Attorney General Gonzales noted that federal judges have reviewed and granted the Department's request for a section 215 order 35 times as of March 30, 2005. To date, the provision has only been used to obtain driver's license records, public accommodations records, apartment leasing records, credit card records, and subscriber information-such as names and addresses-for telephone numbers captured through court-authorized pen registers and trap and trace authority (a pen register records the numbers a telephone dials and a trap and trace device records the numbers from which it receives calls). The Department has not obtained a section 215 order for library or bookstore records, medical records, or gun sale records.

Section 206 gives terrorism investigators the ability to use "roving" wiretaps in their investigations, as criminal investigators have long been able to do. If an international terrorism suspect were to switch his cell phone provider each week, national security investigators are now able to continue tracking him under section 206, because their court-authorized wiretap would cover the individual and not just one cell phone that the suspect might discard after a short time.

Prior to the passage of the PATRIOT Act, every time an international terrorist or spy changed cell phones or switched communications providers, investigators had to return to court to obtain a new surveillance order, leaving open the possibility that they might miss a key conversation that could help them prevent a terrorist attack or protect American lives. Section 206 of the PATRIOT Act fixed this problem by authorizing multi-point or "roving" surveillance of an international terrorist or spy when a federal judge finds that the target may act to throw investigators off his trail. This section has been used 49 times as of March 30, 2005 and proven effective in monitoring spies and international terrorists.

Other sections of the USA PATRIOT Act have also helped in the fight against terrorism. For example, section 207 increased the initial time duration for Foreign Intelligence Surveillance Act (FISA) electronic surveillance and physical search orders and the Department estimates that it has saved nearly 60,000 attorney-hours-nearly a year's worth of work for 30 Department attorneys. Section 207 includes provisions that apply to orders targeting foreigners who act inside the United States as officers and employees of a foreign power and members of a group engaged in international terrorism as well as other provisions that apply to both U.S. persons and non-U.S. persons. Attorney General Gonzales today proposed that the FISA process be further improved by increasing the maximum time duration of: (1) surveillance and search orders targeting any agent of a foreign power who is not a U.S. person; and (2) pen register orders-in

cases where the information obtained is likely to involve foreign intelligence not concerning a U.S. person.

Most of these ideas regarding section 207 were endorsed by the bipartisan Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, which said that they would help Justice Department personnel to "focus their attention where it is most needed." These changes would have saved the Department an estimated 25,000 additional attorney-hours had they been in effect since the passage of the USA PATRIOT Act.

In certain narrow cases, the PATRIOT Act allows courts to give delayed notice that a search warrant has been executed. Delayed-notification warrants-codified by section 213-are a longstanding crime-fighting tool that courts across the country have upheld for decades. While this provision will not sunset, Attorney General Gonzales today emphasized the importance of this section, which always requires a judge's approval and notice to a person whose property is searched. In appropriate cases, delayed-notification searches are necessary because, if terrorists or other criminals are prematurely tipped off that they are under investigation, they could take actions such as destroying evidence, harming witnesses, or fleeing prosecution.

The Justice Department announced yesterday that since the PATRIOT Act set uniform nationwide standards for the issuance of delayed-notification search warrants, the Department has been authorized to use them 155 times as of January 31, 2005. The Department estimates that court-approved delayed-notification warrants represent less than 0.2 percent of the search warrants handled by the federal courts.

The law enforcement tools provided by the PATRIOT Act have been an important part of many of the nation's counterterrorism successes, including helping to charge 379 defendants with terrorism-related crimes and attaining more than 200 convictions or guilty pleas. In addition to providing tools that have been instrumental in the war on terror, the USA PATRIOT Act tore down the "wall" between the law enforcement and intelligence communities, allowing them to share information and "connect the dots" to uncover terrorist plots before they are completed.

###

05-161

****

STATEMENT OF ALBERTO R. GONZALES
ATTORNEY GENERAL OF THE UNITED STATES
BEFORE THE UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY
APRIL 5, 2005

Chairman Specter, Ranking Member Leahy, and Members of the Committee:

It is my pleasure to appear before you this morning to discuss the USA PATRIOT Act. Approximately three-and-a-half years ago, our Nation suffered a great tragedy. Thousands of our fellow citizens were murdered at the World Trade Center, the Pentagon, and a field in rural Pennsylvania. We will never forget that day or the heroes who perished on that hallowed ground. Forever in our Nation's collective memory are stories of the New York City firefighters who rushed into burning buildings so that others might live and of the brave passengers who brought down United Airlines Flight 93 before it could reach Washington, DC, and the messages from those trapped in the World Trade Center saying their last goodbyes to loved ones as they faced certain death will stay forever in our hearts.

In the wake of this horrific attack on American soil, we mourned our Nation's terrible loss. In addition, we came together in an effort to prevent such a tragedy from ever happening again. Members of both parties worked together on legislation to ensure that investigators and prosecutors would have the tools they need to uncover and disrupt terrorist plots. Additionally, members joined hands across the aisle to guarantee that our efforts to update and strengthen the laws governing the investigation and prosecution of terrorism remained firmly within the parameters of the Constitution and our fundamental national commitment to the protection of civil rights and civil liberties.

The result of this collaboration was the USA PATRIOT Act, which passed both Houses of the Congress with overwhelming bipartisan majorities and was signed into law by President Bush on October 26, 2001. In the past three-and-a-half years, the USA PATRIOT Act has been an integral part of the Federal Government's successful prosecution of the war against terrorism. Thanks to the Act, we have been able to

identify terrorist operatives, dismantle terrorist cells, disrupt terrorist plots, and capture terrorists before they have been able to strike.

Many of the most important provisions of the USA PATRIOT Act, however, are scheduled to expire at the end of this year. Therefore, I am here today primarily to convey one simple message: All provisions of the USA PATRIOT Act that are scheduled to sunset at the end of this year must be made permanent. While we have made considerable progress in the war against terrorism in the past three-and-a-half years, al Qaeda and other terrorist groups still pose a grave threat to the safety and security of the American people. The tools contained in the USA PATRIOT Act have proven to be essential weapons in our arsenal to combat the terrorists, and now is not the time for us to be engaging in unilateral disarmament. Moreover, many provisions in the Act simply updated the law to reflect recent technological developments and have been used, as was intended by Congress, not only in terrorism cases, but also to combat other serious criminal conduct. If these provisions are not renewed, the Department's ability to combat serious offenses such as cybercrime, child pornography, and kidnappings will also be hindered.

As Congress considers whether to renew key USA PATRIOT Act provisions, I also wish to stress that I am open to any ideas that may be offered for improving these provisions. If members of this Committee or other members of Congress wish to offer proposals in this regard, I and others at the Department of Justice would be happy to consult with you and review your ideas. However, let me be clear about one thing: I will not support any proposal that would undermine the ability of investigators and prosecutors to disrupt terrorist plots and combat terrorism effectively.

It is also my sincere hope that we will be able to consider these crucial issues in a calm and thoughtful fashion. All of us seek to ensure the safety and security of the American people and to protect their civil liberties as well. As this debate goes forward, I will treat those who express concerns about the USA PATRIOT Act with respect and listen to their concerns with an open mind. I also hope that all who participate in the debate will stick to the facts and avoid overheated rhetoric that inevitably tends to obfuscate rather than elucidate the truth.

Today, I would like to use the rest of my testimony to explain how key provisions of the USA PATRIOT Act have helped to protect the American people. I will particularly focus on those sections of the Act that are scheduled to expire at the end of 2005. To begin with, I will discuss how the USA PATRIOT Act has enhanced the federal government's ability to share intelligence. Then, I will explain how the USA PATRIOT Act provided terrorism investigators with many of the same tools long available to investigators in traditional criminal cases. Additionally, I will explore how the USA PATRIOT Act updated the law to reflect new technology. And finally, I will review how the Act protects the civil liberties of the American people and respects the important role of checks and balances within the Federal Government.

Information Sharing

The most important reforms contained in the USA PATRIOT Act improved coordination and information sharing within the Federal Government. Prior to the attacks of September 11, 2001, our counterterrorism efforts were severely hampered by unnecessary obstacles and barriers to information sharing. These obstacles and barriers, taken together, have been described as a "wall" that largely separated intelligence

personnel from law enforcement personnel, thus dramatically hampering the Department's ability to detect and disrupt terrorist plots.

It is vitally important for this Committee to understand how the "wall" was developed and how it was dismantled, not for the purpose of placing blame but rather to ensure that it is never rebuilt. Before the passage of the USA PATRIOT Act, the Foreign Intelligence Surveillance Act (FISA) mandated that applications for orders authorizing electronic surveillance or physical searches under FISA were required to include a certification that "the purpose" of the surveillance or search was to gather foreign intelligence information. This requirement, however, came to be interpreted by the courts and later the Department of Justice to require that the "primary purpose" of the collection was to obtain foreign intelligence information rather than evidence of a crime. And, because the courts evaluated the Department's purpose for using FISA, in part, by examining the nature and extent of coordination between intelligence and law enforcement personnel, the more coordination that occurred, the more likely courts would find that law enforcement, rather than foreign intelligence, had become the primary purpose of the surveillance or search, a finding that would prevent the court from authorizing surveillance under FISA. As a result, over the years, the "primary purpose" standard had the effect of constructing a metaphorical "wall" between intelligence and law enforcement personnel.

During the 1980s, a set of largely unwritten rules only limited information sharing between intelligence and law enforcement officials to some degree. In 1995, however, the Department established formal procedures that limited the sharing of information between intelligence and law enforcement personnel. The promulgation of these

procedures was motivated in part by the concern that the use of FISA authorities would not be allowed to continue in particular investigations if criminal prosecution began to overcome intelligence gathering as an investigation's primary purpose.

As they were originally designed, the procedures were intended to permit a degree of interaction and information sharing between prosecutors and intelligence officers, while at the same time ensuring that the FBI would be able to obtain or continue FISA surveillance and later use the fruits of that surveillance in a criminal prosecution. Over time, however, coordination and information sharing between intelligence and law enforcement investigators became even more limited in practice than was permitted in theory. Due both to the complexities of the restrictions on information sharing and to a perception that improper information sharing could end a career, investigators often erred on the side of caution and refrained from sharing information. The end result was a culture within the Department sharply limiting the exchange of information between intelligence and law enforcement officials.

In hindsight, it is difficult to overemphasize the negative impact of the "wall." In order to uncover terrorist plots, it is essential that investigators have access to as much information as possible. Often, only by piecing together disparate and seemingly unrelated points of information are investigators able to detect suspicious patterns of activity, a phenomenon generally referred to as "connecting the dots." If, however, one set of investigators has access to only one-half of the dots, and another set of investigators has access to the other half of the dots, the likelihood that either set of investigators will be able to connect the dots is significantly reduced.

The operation of the "wall" was vividly illustrated in testimony from Patrick

Fitzgerald, U.S. Attorney for the Northern District of Illinois, before the Senate Judiciary Committee:

> I was on a prosecution team in New York that began a criminal investigation of Usama Bin Laden in early 1996. The team - prosecutors and FBI agents assigned to the criminal case - had access to a number of sources. We could talk to citizens. We could talk to local police officers. We could talk to other U.S. Government agencies. We could talk to foreign police officers. Even foreign intelligence personnel. And foreign citizens. And we did all those things as often as we could. We could even talk to al Qaeda members - and we did. We actually called several members and associates of al Qaeda to testify before a grand jury in New York. And we even debriefed al Qaeda members overseas who agreed to become cooperating witnesses.
>
> But there was one group of people we were not permitted to talk to. Who? The FBI agents across the street from us in lower Manhattan assigned to a parallel intelligence investigation of Usama Bin Laden and al Qaeda. We could not learn what information they had gathered. That was "the wall."

Thanks in large part to the USA PATRIOT Act, this "wall" has been lowered. Section 218 of the Act, in particular, helped to tear down the "wall" by eliminating the "primary purpose" requirement under FISA and replacing it with a "significant purpose" test. Under section 218, the Department may now conduct FISA surveillance or searches if foreign-intelligence gathering is a "significant purpose" of the surveillance or search. As a result, courts no longer need to compare the relative weight of the "foreign intelligence" and "law enforcement" purposes of a proposed surveillance or search and determine which is the primary purpose; they simply need to determine whether a significant purpose of the surveillance is to obtain foreign intelligence. The consequence is that intelligence and law enforcement personnel may share information much more freely without fear that such coordination will undermine the Department's ability to continue to gain authorization for surveillance under FISA.

Section 218 of the USA PATRIOT Act not only removed what was perceived at

the time as the primary impediment to robust information sharing between intelligence and law enforcement personnel; it also provided the necessary impetus for the removal of the formal administrative restrictions as well as the informal cultural restrictions on information sharing. Thanks to the USA PATRIOT Act, the Department has been able to move from a culture where information sharing was viewed with a wary eye to one where it is an integral component of our counterterrorism strategy. Following passage of the Act, the Department adopted new procedures specifically designed to increase information sharing between intelligence and law enforcement personnel. Moreover, Attorney General Ashcroft instructed every U.S. Attorney across the country to review intelligence files to discover whether there was a basis for bringing criminal charges against the subjects of intelligence investigations. He also directed every U.S. Attorney to develop a plan to monitor intelligence investigations, to ensure that information about terrorist threats is shared with other agencies, and to consider criminal charges in those investigations.

The increased information sharing facilitated by section 218 of the USA PATRIOT Act has led to tangible results in the war against terrorism: plots have been disrupted; terrorists have been apprehended; and convictions have been obtained in terrorism cases. Information sharing between intelligence and law enforcement personnel, for example, was critical in successfully dismantling a terror cell in Portland, Oregon, popularly known as the "Portland Seven," as well as a terror cell in Lackawanna, New York. Such information sharing has also been used in the prosecution of: several persons involved in al Qaeda drugs-for-weapons plot in San Diego, two of whom have pleaded guilty; nine associates in Northern Virginia of a violent extremist group known

as Lashkar-e-Taiba that has ties to al Qaeda, who were convicted and sentenced to prison terms ranging from four years to life imprisonment; two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Mohshen Yahya Zayed, who were charged and convicted for conspiring to provide material support to al Qaeda and HAMAS; Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq as well as two counts of perjury; and Enaam Arnaout, the Executive Director of the Illinois-based Benevolence International Foundation, who had a long-standing relationship with Osama Bin Laden and pleaded guilty to a racketeering charge, admitting that he diverted thousands of dollars from his charity organization to support Islamic militant groups in Bosnia and Chechnya. Information sharing between intelligence and law enforcement personnel has also been extremely valuable in a number of other ongoing or otherwise sensitive investigations that I am not at liberty to discuss today.

While the "wall" primarily blocked the flow of information from intelligence investigators to law enforcement investigators, another set of barriers, before the passage of the USA PATRIOT Act, often prevented law enforcement officials from sharing information with intelligence personnel and others in the government responsible for protecting the national security. Federal law, for example, was interpreted generally to prohibit federal prosecutors from disclosing information from grand jury testimony and criminal investigative wiretaps to intelligence and national defense officials even if that information indicated that terrorists were planning a future attack, unless such officials were actually assisting with the criminal investigation. Sections 203(a) and (b) of the USA PATRIOT Act, however, eliminated these obstacles to information sharing by

allowing for the dissemination of that information to assist Federal law enforcement, intelligence, protective, immigration, national defense, and national security officials in the performance of their official duties, even if their duties are unrelated to the criminal investigation. (Section 203(a) covers grand jury information, and section 203(b) covers wiretap information). Section 203(d), likewise, ensures that important information that is obtained by law enforcement means may be shared with intelligence and other national security officials. This provision does so by creating a generic exception to any other law purporting to bar Federal law enforcement, intelligence, immigration, national defense, or national security officials from receiving, for official use, information regarding foreign intelligence or counterintelligence obtained as part of a criminal investigation. Indeed, section 905 of the USA PATRIOT Act requires the Attorney General to expeditiously disclose to the Director of Central Intelligence foreign intelligence acquired by the Department of Justice in the course of a criminal investigation unless disclosure of such information would jeopardize an ongoing investigation or impair other significant law enforcement interests.

The Department has relied on section 203 in disclosing vital information to the intelligence community and other federal officials on many occasions. Such disclosures, for instance, have been used to assist in the dismantling of terror cells in Portland, Oregon and Lackawanna, New York, to support the revocation of suspected terrorists' visas, to track terrorists' funding sources, and to identify terrorist operatives overseas.

The information sharing provisions described above have been heralded by investigators in the field as the most important provisions of the USA PATRIOT Act. Their value has also been recognized by the 9/11 Commission, which stated in its official

report that "[t]he provisions in the act that facilitate the sharing of information among intelligence agencies and between law enforcement and intelligence appear, on balance, to be beneficial."

Since the passage of the USA PATRIOT Act, Congress has taken in the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act of 2004 other important steps forward to improve coordination and information sharing throughout the Federal Government. If Congress does not act by the end of the year, however, we will soon take a dramatic step back to the days when unnecessary obstacles blocked vital information sharing. Three of the key information sharing provisions of the USA PATRIOT Act, sections 203(b), 203(d), and 218, are scheduled to sunset at the end of the year. It is imperative that we not allow this to happen. To ensure that the "wall" is not reconstructed and investigators are able to "connect the dots" to prevent future terrorist attacks, these provisions must be made permanent.

Using Preexisting Tools in Terrorism Investigations

In addition to enhancing the information sharing capabilities of the Department, the USA PATRIOT Act also permitted several existing investigative tools that had been used for years in a wide range of criminal investigations to be used in terrorism cases as well. Essentially, these provisions gave investigators the ability to fight terrorism utilizing many of the same court-approved tools that have been used successfully and constitutionally for many years in drug, fraud, and organized crime cases.

Section 201 of the USA PATRIOT Act is one such provision. In the context of criminal law enforcement, Federal investigators have long been able to obtain court orders to conduct wiretaps when investigating numerous traditional criminal offenses.

Specifically, these orders have authorized the interception of certain communications to investigate the predicate offenses listed in the federal wiretap statute, 18 U.S.C. § 2516(1). The listed offenses include numerous crimes, such as drug crimes, mail fraud, passport fraud, embezzlement from pension and welfare funds, the transmission of wagering information, and obscenity offenses.

Prior to the passage of the USA PATRIOT Act, however, certain extremely serious crimes that terrorists are likely to commit were not included in this list, which prevented law enforcement authorities from using wiretaps to investigate these serious terrorism-related offenses. As a result, law enforcement could obtain under appropriate circumstances a court order to intercept phone communications in a passport fraud investigation but not a chemical weapons investigation or an investigation into terrorism transcending national boundaries.

Section 201 of the Act ended this anomaly in the law by amending the criminal wiretap statute to add the following terrorism-related crimes to the list of wiretap predicates: (1) chemical-weapons offenses; (2) certain homicides and other acts of violence against Americans occurring outside of the country; (3) the use of weapons of mass destruction; (4) acts of terrorism transcending national borders; (5) financial transactions with countries which support terrorism; and (6) material support of terrorists and terrorist organizations.

This provision simply enables investigators to use wiretaps when looking into the full range of terrorism-related crimes. This authority makes as much, if not more, sense in the war against terrorism as it does in traditional criminal investigations; if wiretaps are an appropriate investigative tool to be utilized in cases involving bribery, gambling, and

obscenity, then surely investigators should be able to use them when investigating the use of weapons of mass destruction, acts of terrorism transcending national borders, chemical weapons offenses, and other serious crimes that terrorists are likely to commit.

It is also important to point out that section 201 preserved all of the pre-existing standards in the wiretap statute. For example, law enforcement must file an application with a court, and a court must find that: (1) there is probable cause to believe an individual is committing, has committed, or is about to commit a particular predicate offense; (2) there is probable cause to believe that particular communications concerning that offense will be obtained through the wiretap; and (3) "normal investigative procedures" have been tried and failed or reasonably appear to be unlikely to succeed or are too dangerous.

Section 206 of the USA PATRIOT Act, like section 201 discussed above, provided terrorism investigators with an authority that investigators have long possessed in traditional criminal investigations. Before the passage of the Act, multipoint or so-called "roving" wiretap orders, which attach to a particular suspect rather than a particular phone or communications facility, were not available under FISA. As a result, each time an international terrorist or spy switched communications providers, for example, by changing cell phones or Internet accounts, investigators had to return to court to obtain a new surveillance order, often leaving investigators unable to monitor key conversations.

Congress eliminated this problem with respect to traditional criminal crimes, such as drug offenses and racketeering, in 1986 when it authorized the use of multi-point or "roving" wiretaps in criminal investigations. But from 1986 until the passage of the USA

PATRIOT Act in 2001, such authority was not available under FISA for cases involving terrorists and spies. Multi-point wiretaps could be used to conduct surveillance of drug dealers but not international terrorists. However, such authority was needed under FISA. International terrorists and foreign intelligence officers are trained to thwart surveillance by changing the communications facilities they use, thus making vital the ability to obtain "roving" surveillance. Without such surveillance, investigators were often left two steps behind sophisticated terrorists.

Section 206 of the Act amended the law to allow the FISA Court to authorize multi-point surveillance of a terrorist or spy when it finds that the target's actions may thwart the identification of those specific individuals or companies, such as communications providers, whose assistance may be needed to carry out the surveillance. Thus, the FISA Court does not have to name in the wiretap order each telecommunications company or other "specified person" whose assistance may be required.

A number of federal courts - including the Second, Fifth, and Ninth Circuits - have squarely ruled that multi-point wiretaps are perfectly consistent with the Fourth Amendment. Section 206 simply authorizes the same constitutional techniques used to investigate ordinary crimes to be used in national-security investigations. Despite this fact, section 206 remains one of the more controversial provisions of the USA PATRIOT Act. However, as in the case of multi-point wiretaps used for traditional criminal investigations, section 206 contains ample safeguards to protect the privacy of innocent Americans.

First, section 206 did not change FISA's requirement that the target of multi-point

surveillance must be identified or described in the order. In fact, section 206 is always connected to a particular target of surveillance. For example, even if the Justice Department is not sure of the actual identity of the target of such a wiretap, FISA nonetheless requires our attorneys to provide a description of the target of the electronic surveillance to the FISA Court prior to obtaining multi-point surveillance order.

Second, just as the law required prior to the Act, the FISA Court must find that there is probable cause to believe the target of surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or spy. In addition, the FISA Court must also find that the actions of the target of the application may have the effect of thwarting surveillance before multi-point surveillance may be authorized.

Third, section 206 in no way altered the robust FISA minimization procedures that limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons.

Section 214 is yet another provision of the USA PATRIOT Act that provides terrorism investigators with the same authority that investigators have long possessed in traditional criminal investigations. Specifically, this section allows the government to obtain a pen register or trap-and-trace order in national security investigations where the information to be obtained is likely to be relevant to an international terrorism or espionage investigation. A pen register or trap-and-trace device can track routing and addressing information about a communication - for example, which numbers are dialed from a particular telephone. Such devices, however, are not used to collect the content of communications.

Under FISA, intelligence officers may seek a court order for a pen register or

trap-and-trace to gather foreign intelligence information or information about international terrorism. Prior to the enactment of the USA PATRIOT Act, however, FISA required government personnel to certify not just that the information they sought to obtain with a pen register or trap-and-trace device would be relevant to their investigation, but also that the particular facilities being monitored, such as phones, were being used by foreign governments, international terrorists, or spies. As a result, it was much more difficult to obtain a pen register or trap-and-trace device order under FISA than it was under the criminal wiretap statute, where the applicable standard was and remains simply one of relevance in an ongoing criminal investigation.

Section 214 of the Act simply harmonized the standard for obtaining a pen register order in a criminal investigation and a national-security investigation by eliminating the restriction limiting FISA pen register and trap-and-trace orders to facilities used by foreign agents or agents of foreign powers. Applicants must still, however, certify that a pen register or trap-and-trace device is likely to reveal information relevant to an international terrorism or espionage investigation or foreign intelligence information not concerning a United States person. This provision made the standard contained in FISA for obtaining a pen register or trap-and-trace order parallel with the standard for obtaining those same orders in the criminal context. Now, as before, investigators cannot install a pen register or trap-and-trace device unless they apply for and receive permission from the FISA Court.

I will now turn to section 215, which I recognize has become the most controversial provision in the USA PATRIOT Act. This provision, however, simply granted national security investigators the same authority that criminal investigators have

had for centuries - that is, to request the production of records that may be relevant to their investigation. For years, ordinary grand juries have issued subpoenas to obtain records from third parties that are relevant to criminal inquiries. But just as prosecutors need to obtain such records in order to advance traditional criminal investigations, so, too, must investigators in international terrorism and espionage cases have the ability, with appropriate safeguards, to request the production of relevant records.

While obtaining business records is a long-standing law enforcement tactic that has been considered an ordinary tool in criminal investigations, prior to the USA PATRIOT Act it was difficult for investigators to obtain access to the same types of records in connection with foreign intelligence investigations. Such records, for example, could be sought only from common carriers, public accommodation providers, physical storage facility operators, and vehicle rental agencies. In addition, intelligence investigators had to meet a higher evidentiary standard to obtain an order requiring the production of such records than prosecutors had to meet to obtain a grand jury subpoena to require the production of those same records in a criminal investigation.

To address this anomaly in the law, section 215 of the Act made several important changes to the FISA business-records authority so that intelligence agents would be better able to obtain crucial information in important national-security investigations. Section 215 expanded the types of entities that can be compelled to disclose information. Under the old provision, the FBI could obtain records only from "a common carrier, public accommodation facility, physical storage facility or vehicle rental facility." The new provision contains no such restrictions. Section 215 also expanded the types of items that can be requested. Under the old authority, the FBI could only seek "records." Now, the

FBI can seek "any tangible things (including books, records, papers, documents, and other items)."

I recognize that section 215 has been subject to a great deal of criticism because of its speculative application to libraries, and based on what some have said about the provision, I can understand why many Americans would be concerned. The government should not be obtaining the library records of law-abiding Americans, and I will do everything within my power to ensure that this will not happen on my watch.

Section 215 does not focus on libraries. Indeed, the USA PATRIOT Act nowhere mentions the word "library," a fact that many Americans are surprised to learn. Section 215 simply does not exempt libraries from the range of entities that may be required to produce records. Now some have suggested, since the Department has no interest in the reading habits of law-abiding Americans, that section 215 should be amended to forbid us from using the provision to request the production of records from libraries and booksellers. This, however, would be a serious mistake.

Libraries are currently not safe havens for criminals. Grand jury subpoenas have long been used to obtain relevant records from libraries and bookstores in criminal investigations. In fact, law enforcement used this authority in investigating the Gianni Versace murder case as well as the case of the Zodiac gunman in order to determine who checked out particular books from public libraries that were relevant in those murder investigations. And if libraries are not safe havens for common criminals, neither should they be safe havens for international terrorists or spies, especially since we know that terrorists and spies have used libraries to plan and carry out activities that threaten our national security. The Justice Department, for instance, has confirmed that, as recently as

the winter and spring of 2004, a member of a terrorist group closely affiliated with al Qaeda used Internet service provided by a public library to communicate with his confederates.

Section 215, moreover, contains very specific safeguards in order to ensure that the privacy of law-abiding Americans, both with respect to their library records as well as other types of records, is respected. First, section 215 expressly protects First Amendment rights, unlike grand jury subpoenas. Even though libraries and bookstores are not specifically mentioned in the provision, section 215 does prohibit the government from using this authority to conduct investigations "of a United States person solely on the basis of activities protected by the First Amendment to the Constitution of the United States." In other words, the library habits of ordinary Americans are of no interest to those conducting terrorism investigations, nor are they permitted to be.

Second, any request for the production of records under section 215 must be issued through a court order. Therefore, investigators cannot use this authority unilaterally to compel any entity to turn over its records; rather, a judge must first approve the government's request. By contrast, a grand jury subpoena is typically issued without any prior judicial review or approval. Both grand jury subpoenas and section 215 orders are also governed by a standard of relevance. Under section 215, agents may not seek records that are irrelevant to an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

Third, section 215 has a narrow scope. It can only be used in an authorized investigation (1) "to obtain foreign intelligence information not concerning a United

States person"; or (2) "to protect against international terrorism or clandestine intelligence activities." It cannot be used to investigate ordinary crimes, or even domestic terrorism. On the other hand, a grand jury many obtain business records in investigations of *any* federal crime.

Finally, section 215 provides for thorough congressional oversight that is not present with respect to grand-jury subpoenas. On a semi-annual basis, I must "fully inform" appropriate congressional committees concerning all requests for records under section 215 as well as the number of section 215 orders granted, modified, or denied. To date, the Department has provided Congress with six reports regarding its use of section 215.

Admittedly, the recipient of an order under section 215 is not permitted to make that order publicly known, and this confidentiality requirement has generated some fear among the public. It is critical, however, that terrorists are not tipped off prematurely about sensitive investigations. Otherwise, their conspirators may flee and key information may be destroyed before the government's investigation has been completed. As the U.S. Senate concluded when adopting FISA: "By its very nature, foreign intelligence surveillance must be conducted in secret."

Updating the Law To Reflect New Technology

As well as providing terrorism investigators many of the same tools that law enforcement investigators had long possessed in traditional criminal investigations, many sections of the USA PATRIOT Act updated the law to reflect new technology and to prevent sophisticated terrorists and criminals from exploiting that new technology. Several of these provisions, some of which are currently set to sunset at the end of this

year, simply updated tools available to law enforcement in the context of ordinary criminal investigations to address recent technological developments, while others sought to make existing criminal statutes technology-neutral. I wish to focus on five such provisions of the Act, which are currently set to expire at the end of 2005. The Department believes that each of these provisions has proven valuable and should be made permanent.

Section 212 amended the Electronic Communications Privacy Act to authorize electronic communications service providers to disclose communications and records relating to customers or subscribers in an emergency involving the immediate danger of death or serious physical injury. Before the USA PATRIOT Act, for example, if an Internet service provider had learned that a customer was about to commit a terrorist act and notified law enforcement to that effect, the service provider could have been subject to civil lawsuits. Now, however, providers are permitted voluntarily to turn over information to the government in emergencies without fear of civil liability. It is important to point out that they are under no obligation whatsoever to review customer communications and records. This provision also corrected an anomaly in prior law under which an Internet service provider could voluntarily disclose the content of communications to protect itself against hacking, but could not voluntarily disclose customer records for the same purpose.

Communications providers have relied upon section 212 to disclose vital and time-sensitive information to the government on many occasions since the passage of the USA PATRIOT Act, thus saving lives. To give just one example, this provision was used to apprehend an individual threatening to destroy a Texas mosque before he could

carry out his threat. Jared Bjarnason, a 30-year-old resident of El Paso, Texas, sent an e-mail message to the El Paso Islamic Center on April 18, 2004, threatening to burn the Islamic Center's mosque to the ground if hostages in Iraq were not freed within three days. Section 212 allowed FBI officers investigating the threat to obtain information quickly from electronic communications service providers, leading to the identification and arrest of Bjarnason before he could attack the mosque. It is not clear, however, that absent section 212 investigators would have been able to locate and apprehend Bjarnason in time.

Section 212 of the USA PATRIOT Act governed both the voluntary disclosure of the content of communications and the voluntary disclosure of non-content customer records in emergency situations; but in 2002, the Homeland Security Act repealed that portion of section 212 governing the disclosure of the content of communications in emergency situations and placed similar authority in a separate statutory provision that is not scheduled to sunset. The remaining portion of section 212, governing the disclosure of customer records, however, is set to expire at the end of 2005. Should section 212 expire, communications providers would be able to disclose the content of customers' communications in emergency situations but would not be able voluntarily to disclose non-content customer records pertaining to those communications. Such an outcome would defy common sense. Allowing section 212 to expire, moreover, would dramatically restrict communications providers' ability voluntarily to disclose life-saving information to the government in emergency situations.

Section 202, for its part, modernized the criminal code in light of the increased importance of telecommunications and digital communications. The provision allows

law enforcement to use pre-existing wiretap authorities to intercept voice communications, such as telephone conversations, in the interception of felony offenses under the Computer Fraud and Abuse Act. These include many important cybercrime and cyberterrorism offenses, such as computer espionage and intentionally damaging a Federal Government computer. Significantly, section 202 preserved all of the pre-existing standards in the wiretap statute, meaning that law enforcement must file an application with a court, and a court must find that: (1) there is probable cause to believe an individual is committing, has committed, or is about to commit a particular predicate offense; (2) there is probable cause to believe that particular communications concerning that offense will be obtained through the wiretap; and (3) "normal investigative procedures" have been tried and failed or reasonably appear to be unlikely to succeed or are too dangerous. If wiretaps are an appropriate investigative tool to be utilized in cases involving bribery, gambling, and obscenity, as was the case prior to the passage of the USA PATRIOT Act, then surely investigators should be able to use them when investigating computer espionage, extortion, and other serious cybercrime and cyberterrorism offenses.

Turning to section 220, that provision allows courts, in investigations over which they have jurisdiction, to issue search warrants for electronic evidence stored outside of the district where they are located. Federal law requires investigators to use a search warrant to compel an Internet service provider to disclose unopened e-mail messages that are less than six months old. Prior to the USA PATRIOT Act, some courts interpreting Rule 41 of the Federal Rules of Criminal Procedure declined to issue search warrants for e-mail messages stored on servers in other districts, leading to delays in many time-

sensitive investigations as investigators had to bring agents, prosecutors, and judges in another district up to speed. Requiring investigators to obtain warrants in distant jurisdictions also placed enormous administrative burdens on districts in which major Internet service providers are located, such as the Northern District of California and the Eastern District of Virginia.

Section 220 fixed this problem. It makes clear, for example, that a judge with jurisdiction over a murder investigation in Pennsylvania can issue a search warrant for e-mail messages pertaining to that investigation that were stored on a server in Silicon Valley. Thus, investigators in Pennsylvania, under this scenario, can ask a judge familiar with the investigation to issue the warrant rather than having to ask Assistant United States Attorneys in California, who are unfamiliar with the case, to ask a judge in the United States District Court for the Northern District of California, who is also unfamiliar with the case, to issue the warrant.

The Department has already utilized section 220 in important terrorism investigations. As Assistant Attorney General Christopher Wray testified before this committee on October 21, 2003, section 220 was useful in the Portland terror cell case because "the judge who was most familiar with the case was able to issue the search warrants for the defendants' e-mail accounts from providers in other districts, which dramatically sped up the investigation and reduced all sorts of unnecessary burdens on other prosecutors, agents and courts." This section has been similarly useful in the "Virginia Jihad" case involving a Northern Virginia terror cell and in the case of the infamous "shoebomber" terrorist Richard Reid. Moreover, the ability to obtain search warrants in the jurisdiction of the investigation has proven critical to the success of

complex, multi-jurisdictional child pornography cases.

Contrary to concerns voiced by some, section 220 does not promote forum-shopping; the provision may be used only in a court with jurisdiction over the investigation. Investigators may not ask any court in the country to issue a warrant to obtain electronic evidence.

It is imperative that section 220 be renewed; allowing the provision to expire would delay many time-sensitive investigations and result in the inefficient use of investigators', prosecutors', and judges' time.

Moving to section 209, that provision made existing statutes technology-neutral by providing that voicemail messages stored with a third-party provider should be treated like e-mail messages and answering machine messages, which may be obtained through a search warrant. Previously, such messages fell under the rubric of the more restrictive provisions of the criminal wiretap statute, which apply to the interception of live conversations. Given that stored voice communications possess few of the sensitivities associated with the real-time interception of telephone communications, it was unreasonable to subject attempts to retrieve voice-mail message stored with third-party providers to the same burdensome process as requests for wiretaps. Section 209 simply allows investigators, upon a showing of probable cause, to apply for and receive a court-ordered search warrant to obtain voicemails held by a third-party provider, preserving all of the pre-existing standards for the availability of search warrants. Since the passage of the USA PATRIOT Act, such search warrants have been used in a variety of criminal cases to obtain key evidence, including voicemail messages left for foreign and domestic terrorists, and to investigate a large-scale Ecstasy smuggling ring based in the

Netherlands.

The speed with which voicemail is seized and searched can often be critical to an investigation given that deleted messages are lost forever. Allowing section 209 to expire, as it is set to do in 2005, would once again require different treatment for stored voicemail messages than for messages stored on an answering machine in a person's home, needlessly hampering law enforcement efforts to investigate crimes and obtain evidence in a timely manner.

Section 217 similarly makes criminal law technology-neutral, placing cyber-trespassers on the same footing as physical intruders by allowing victims of computer-hacking crimes voluntarily to request law enforcement assistance in monitoring trespassers on their computers. Just as burglary victims have long been able to invite officers into their homes to catch the thieves, hacking victims can now invite law enforcement assistance to assist them in combating cyber-intruders. Section 217 does not require computer operators to involve law enforcement if they detect trespassers on their systems; it simply gives them the option to do so. In so doing, section 217 also preserves the privacy of law-abiding computer users by sharply limiting the circumstances under which section 217 is available. Officers may not agree to help a computer owner unless (1) they are engaged in a lawful investigation; (2) there is reason to believe that the communications will be relevant to that investigation; and (3) their activities will not acquire the communications of non-trespassers. Moreover, the provision amended the wiretap statute to protect the privacy of an Internet service provider's customers by providing a definition of "computer trespasser" which excludes an individual who has a contractual relationship with the service provider. Therefore, for example, section 217

would not allow Earthlink to ask law enforcement to help monitor a hacking attack on its system that was initiated by one of its own subscribers.

Since its enactment, section 217 has played a key role in sensitive national security matters, including investigations into hackers' attempts to compromise military computer systems. Section 217 is also particularly helpful when computer hackers launch massive "denial of service" attacks - which are designed to shut down individual web sites, computer networks, or even the entire Internet. Allowing section 217 to expire, which is set to occur in 2005, would lead to a bizarre world in which a computer hacker's supposed privacy right would trump the legitimate privacy rights of a hacker's victims, making it more difficult to combat hacking and cyberterrorism effectively.

Protecting Civil Liberties

While the USA PATRIOT Act provided investigators and prosecutors with tools critical for protecting the American people, it is vital to note that it did so in a manner fully consistent with constitutional rights of the American people. In section 102 of the USA PATRIOT Act, Congress expressed its sense that "the civil rights and civil liberties of all Americans . . . must be protected," and the USA PATRIOT Act does just that.

In the first place, the USA PATRIOT Act contains several provisions specifically designed to provide additional protection to the civil rights and civil liberties of all Americans. Section 223, for example, allows individuals aggrieved by any willful violation of the criminal wiretap statute (Title III), the Electronic Communications Privacy Act, or certain provisions the FISA, to file an action in United States District Court to recover not less than $10,000 in damages. This provision allows an individual whose privacy is violated to sue the United States for money damages if Federal officers

or employees disclose sensitive information without lawful authorization. Section 223 also requires Federal departments and agencies to initiate a proceeding to determine whether disciplinary action is warranted against an officer or employee whenever a court or agency finds that the circumstances surrounding a violation of Title III raise serious questions about whether that officer or employee willfully or intentionally violated Title III. To date, there have been no administrative disciplinary proceedings or civil actions initiated under section 223 of the USA PATRIOT Act. I believe that this reflects the fact that employees of the Justice Department consistently strive to comply with their legal obligations. Nevertheless, section 223 provides an important mechanism for holding the Department of Justice accountable, and I strongly urge Congress not to allow it to sunset at the end of 2005.

Additionally, section 1001 of the USA PATRIOT Act requires the Justice Department's Inspector General to designate one official responsible for the review of complaints alleging abuses of civil rights and civil liberties by Justice Department employees. This individual is then responsible for conducting a public awareness campaign through the Internet, radio, television, and newspaper advertisements to ensure that individuals know how to file complaints with the Office of the Inspector General. Section 1001 also directs the Office of Inspector General to submit to this Committee and the House Judiciary Committee on a semi-annual basis a report detailing any abuses of civil rights and civil liberties by Department employees or officials. To date, six such reports have been submitted by the Office of the Inspector General pursuant to section 1001; they were transmitted in July 2002, January 2003, July 2003, January 2004, September 2004, and March 2005. I am pleased to be able to state that the Office of the

Inspector General has not documented in these reports any abuse of civil rights or civil liberties by the Department related to the use of any substantive provision of the USA PATRIOT Act.

In addition to containing special provisions designed to ensure that the civil rights and civil liberties of the American people are respected, the USA PATRIOT Act also respects the vital role of the judiciary by providing for ample judicial oversight to guarantee that the constitutional rights of all Americans are safeguarded and that the important role of checks and balances within our Federal Government is preserved. As reviewed above, under section 214 of the Act, investigators cannot utilize a pen register or trap-and-trace device unless they apply for and receive permission from the FISA Court. Section 215 of the Act requires investigators to obtain a court order to request the production of business records in national security investigations. Section 206 requires the Foreign Intelligence Surveillance Court to approve the use of "roving" surveillance in national security investigations. Sections 201 and 202 require a Federal court to approve the use of a criminal investigative wiretap, and sections 209 and 220 require a Federal court to issue search warrants to obtain evidence in a criminal investigation.

Besides safeguarding the vital role of the judiciary, the USA PATRIOT Act also recognizes the crucial importance of congressional oversight. On a semiannual basis, for example, as noted before, I am required to report to this Committee and the House Judiciary Committee the number of applications made for orders requiring the production of business records under section 215 as well as the number of such orders granted, modified or denied. I am also required to fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence

of the Senate on a semiannual basis concerning all requests for the production of business records under section 215. These reports were transmitted by the Department to the appropriate committees in April 2002, January 2003, September 2003, December 2003, September 2004, and December 2004. Moreover, I am required by statute to submit a comprehensive report on a semiannual basis to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate regarding the Department's use of FISA. These reports contain valuable information concerning the Department's use of USA PATRIOT Act provisions, including sections 207, 214, and 218.

Finally, I would note that the Department has gone to great lengths to respond to congressional concerns about the implementation of the USA PATRIOT Act. The Department has, for example, provided answers to more than 520 oversight questions from Members of Congress regarding the USA PATRIOT Act. In the 108th Congress alone, in fact, the Department sent 100 letters to Congress that specifically addressed the USA PATRIOT Act. The Department also has provided witnesses at over 50 terrorism-related hearings, and its employees have conducted numerous formal and informal briefings with Members and staff on USA PATRIOT Act provisions. In short, the Department has been responsive and will continue to be responsive as Congress considers whether key sections of the USA PATRIOT Act will be made permanent.

Conclusion

In closing, the issues that we are discussing today are absolutely critical to our Nation's future success in the war against terrorism. The USA PATRIOT Act has a proven record of success when it comes to protecting the safety and security of the

American people, and we cannot afford to allow many of the Act's most important provisions to expire at the end of the year. For while we certainly wish that the terrorist threat would disappear on December 31, 2005, we all know that this will not be the case. I look forward to working with the Members of this Committee closely in the weeks and months ahead, listening to your concerns, and joining together again on a bipartisan basis to ensure that those in the field have the tools that they need to effectively prosecute the war against terrorism. I also look forward to answering your questions today.

###

Civil Liberties and the PATRIOT Act

- In the text of the PATRIOT Act, Congress expressed its sense that "**the civil rights and civil liberties of all Americans . . . must be protected,**" and the PATRIOT Act does just that.

- The PATRIOT Act contains **several provisions specifically designed to provide additional protection to the civil rights and civil liberties of all Americans.**

  - Section 223 of the PATRIOT Act allows individuals aggrieved by any **willful violation of Title III or certain sections of FISA to file an action in United States District Court to recover not less than $10,000 in damages.**

  - Section 223 also requires federal departments and agencies to **initiate a proceeding to determine whether disciplinary action is warranted** against an officer or employee whenever a court, department, or agency finds that the circumstances surrounding a violation of Title III raise serious questions about whether that officer or employee willfully or intentionally violated Title III.

  - Section 211 of the PATRIOT Act provides that cable companies may not disclose a customer's selection of video programming without customer approval.

  - Section 316 of the PATRIOT Act allows an owner of property confiscated under any provision of law relating to the confiscation of assets of suspected international terrorists to **contest that confiscation in court.**

  - Section 1001 of the PATRIOT Act requires the Inspector General of the Department of Justice to **designate one official to review information and receive complaints alleging abuses of civil rights and civil liberties** by employees and officials of the Department of Justice.

- The PATRIOT Act provides for **ample judicial oversight** to ensure that the civil rights and civil liberties of all Americans are safeguarded.

  - Section 213 of the PATRIOT Act requires **judicial approval** for a delayed-notification search warrant.

  - Pursuant to Sections 214 and 216 of the PATRIOT Act, investigators cannot obtain a pen register unless they apply for and receive permission from a **federal court.**

RIF

- Section 215 requires investigators to obtain a **court order** to obtain business records, including library records, in national security investigations.

- Any alien detained pursuant to section 412 of the PATROIT Act may **challenge his or her detention in court** by filing a habeas petition.

- Pursuant to section 507 of the PATRIOT Act, investigators must apply for and obtain a **court order** to compel educational institutions to disclose **educational records**.

- Pursuant to section 508 of the PATRIOT Act, investigators must apply for and obtain a **court order** to compel the National Center for Education Statistics to disclose its records.

- The PATRIOT Act provides for **ample congressional oversight** to ensure that the civil rights and civil liberties of all Americans are safeguarded.

  - The Attorney General is required to report to the House Judiciary Committee and Senate Judiciary Committee **every six months** the number of applications made for **orders requiring the production of business records under Section 215** as well as the number of such orders granted, modified or denied.

  - The Attorney General is also required to **fully inform** the House Intelligence Committee and Senate Intelligence Committee **every six months concerning all requests for the production of business records under Section 215.**

  - The Attorney General is required to report to the House Judiciary and Senate Judiciary Committee **every six months the number of aliens taken into custody pursuant to section 412 of the PATRIOT Act, the justification for each alien's detention, and the length of each alien's detention.**

  - The Secretary of the Treasury is required to notify the House Financial Services Committee and the Senate Banking, Housing, and Urban Affairs Committee **within 10 days of any regulatory restrictions imposed to combat money laundering pursuant to section 311 of the PATRIOT Act.**

  - The Office of the Inspector General of the Department of Justice must submit to the House Judiciary Committee and Senate Judiciary Committee **a report every six months detailing any abuses of civil rights and civil liberties by employees or officials of the Department of Justice reported pursuant to Section 1001 of the PATRIOT Act.**

- The PATRIOT Act **protects the First Amendment rights** of American citizens.

  - Section 214 of the Act provides that requests for a FISA **pen register order** directed against United States persons may not be made in conjunction with the investigation of a United States person based solely on activities protected by the First Amendment.

  - Section 215 of the Act provides that requests for a **FISA court order requiring the production of business records, including library records,** may not be made in conjunction with an investigation of a United States person based solely on activities protected by the First Amendment.

  - Section 505 of the Act provides that requests for **confidential communications transaction records, financial reports, and credit information** for intelligence purposes may not be made in conjunction with an investigation of a United States person based solely on activities protected by the First Amendment.