(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE

Date: 06/19/02

To: All Divisions

Attn: Assistant Director;
SAC;
Legat
CDC

From: Office of the General Counsel
Investigative Law Unit, Room 7326
Contact: Investigative Law Unit, [redacted] b2-1

Approved By: Parkinson Larry R/
Steele Charles M
[redacted] b7C-1

Drafted By: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 1/31/03 BY 62033EK/ss b7C-1

Case ID #: 66F-HQ- 1085160(Pending)-57

Title: NEW LEGISLATION
PATRIOT ACT OF 2001
PROVISIONS ADDRESSING INVESTIGATIVE ISSUES

Synopsis: To supplement guidance previously provided on the USA PATRIOT ACT of 2001 by highlighting provisions of the USA PATRIOT Act of 2001 which are of the most immediate interest to FBI investigations.

Reference: 66F-HQ-A1247863 Serial 70
66F-HQ-A1247863 Serial 71
66F-HQ-A1323588 Serial 364

Details:

Background

On October 26, 2001, the President signed the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (otherwise referred to as the "USA PATRIOT Act" or "Patriot Act") which enhances many investigative tools available to the FBI. Over the last several months, the Office of the General Counsel (OGC) has provided guidance to the field on this Act in the form of e-mails, ECs, and presentations/training.

Among the documents provided are a detailed section-by-section analysis of certain provisions of the Act;[1] two separate ECs prepared by OGC's National Security Law Unit, Counsel dated October 26, 2001, entitled "NEW LEGISLATION, REVISIONS TO FCI/IT LEGAL AUTHORITIES, FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)" and "NEW LEGISLATION, REVISIONS TO FBI/IT LEGAL AUTHORITIES, NATIONAL SECURITY LETTERS"; and an EC prepared by OGC's Legal Forfeiture Unit, dated January 11, 2002, entitled "ASSET FORFEITURE MATTER." The purpose of this communication is to consolidate into one document the guidance previously provided and to highlight those provisions of the Patriot Act of greatest interest to FBI investigative efforts.

This EC has been broken down into three sections. Section I, Investigative Tools, addresses the provisions which modify, amend, or create investigative tools which may apply to many types of investigations. Section II, Money Laundering, highlights some of the new crimes and investigative tools aimed at the financial networks of criminal enterprises. The International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001 was incorporated into the Patriot Act and was intended to significantly increase the United States' ability to combat the financing of terrorism. This section of the EC is only intended to summarize some of the highlights of the Act. Additional, more comprehensive guidance will be forthcoming. Section III, New Terrorism Offenses, summarizes some of the important changes in the criminal statutes regarding terrorist offenses. The forfeiture provisions, information sharing provisions, and other national security related provisions were addressed in detail in the aforementioned ECs and therefore will not be covered by this EC.

Many of the investigative tools provided in the Patriot Act are governed by a sunset provision which will result in their expiration on December 31, 2005 unless renewed by Congress.[2] In order to be prepared to justify their renewal, offices are encouraged to keep records of the effective use of these tools. Important information to be maintained includes both the number of times the investigative tool was effectively used and specific information on noteworthy cases.

---

[1]This document was prepared by the Department of Justice and provided via e-mail to all Chief Division Counsels on October 30, 2001.

[2]Title 3 of the Patriot Act, entitled the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, has a slightly different sunset provision in that it will only expire if Congress enacts a joint resolution containing specific language. The result is that the provisions will continue unless Congress acts otherwise.

I. Investigative Tools

Information from Communications Providers

Voice Mail - Law enforcement can now obtain all voice mail which is stored by a communications provider, including unopened voice mail, using the procedures set forth in 18 U.S.C. §2703 (such as a search warrant). This also applies to other wire communications as defined by the statute. Voice messages stored and in the possession of the user, such as an answering machine, are not covered by this statute. Previously the law was vague on the standard required to compel production of a stored voice mail message, leaving the possibility for argument that a wiretap order was required. This tool is set to expire under the sunset provision. See 18 U.S.C. § 2510; 18 U.S.C. § 2703.

Basic Subscriber Information - The list of information law enforcement can obtain with a subpoena was expanded to include records of session times and durations, any temporarily assigned network address, and the means and source of payment that a customer uses to pay for his/her account with a communications provider. 18 U.S.C. § 2703(c).

Nationwide Search Warrants for E-mail - Courts with jurisdiction over an investigation can now issue a search warrant with nationwide jurisdiction to compel the production of information held by a service provider, such as unopened e-mail. Previously, the search warrant had to be issued by a court in the district where the service provider was located. This tool is set to expire under the sunset provision. 18 U.S.C. § 2703.

Clarification of the Cable Act - In the past there were two statutory standards for privacy protection: one governing cable service (47 U.S.C. § 551, the "Cable Service Act"), and the other governing telephone and Internet privacy (18 U.S.C. § 2510, *et seq.* [wiretap statute], 18 U.S.C. § 2701, *et seq:* [ECPA], 18 U.S.C. § 3121 *et seq.* [pen/trap statute]). This opened the door for cable companies which provide telephone and Internet services to argue that the ECPA, wiretap, and pen/trap statutes did not apply to them. The Patriot Act clarified this issue by stating that the ECPA, wiretap, and pen/trap statutes govern disclosures by cable companies that relate to the provision of communication services. See 47 U.S.C. § 551(c)(2)(D).

Voluntary Disclosures - The law now explicitly permits, but does not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure, however, does not create an affirmative obligation to review customer communications in search of such imminent dangers. The Act also allows a communications service provider to disclose non-content records to protect their rights and property. This will most often be used when the

communications service provider itself is a victim of computer hacking. This provision will expire under the sunset provision. See 18 U.S.C. § 2702(b) & (c)(3); 18 U.S.C. § 2703(c)(2)(F).

Electronic Surveillance

Expanded Predicates for Title III - The predicate offenses for Title III were expanded to include crimes relating to chemical weapons (18 U.S.C. § 229), terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B), and felony violations of computer fraud and abuse (18 U.S.C. § 1030). This is set to expire under the sunset provision. See 18 U.S.C. § 2516.

Nationwide Effect of Pen/Trap Orders - The Act amends the pen/trap statute to give federal courts the authority to compel assistance from any provider of communication services in the United States whose assistance is appropriate to effectuate the order. See 18 U.S.C. § 3127(2).

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

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

Intercepting Communications of Computer Trespassers - The wiretap statute was amended to explicitly provide victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. In the past, the law was ambiguous on this point. Before monitoring can occur, however, four requirements must be met. First, consent from the owner or operator of the protected computer must be obtained. Second, law enforcement must be acting pursuant to an ongoing investigation. Both criminal and intelligence

investigations qualify, but the authority to intercept ceases at the conclusion of the investigation. Third, law enforcement must have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. And fourth, investigators must only intercept the communications sent or received by trespassers. Thus, this section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting users authorized to use the computer. Additionally, based on the definition of a "computer trespasser," communications of users who have a contractual relationship with the computer owner may not be monitored, even if their use is in violation of their contract terms (i.e. spammers). This is set to expire under the sunset provision. See 18 U.S.C. § 1030(e)(2); 18 U.S.C. § 2510 (20) & (21); 18 U.S.C. § 2511(2)(i).

Pen Register/Trap and Trace Reporting Requirement - The statute created a new reporting requirement whenever the government uses its own pen register or trap and trace equipment on a packet-switched data network of an electronic communications service to the public. While this provision was aimed at the use of the DCS-1000 (earlier versions were known as Carnivore), it will also apply to the use of other government owned equipment/software, such as Etherpeek, on a service provider's network. While additional detailed guidance will be forthcoming, this new requirement imposes a duty to maintain records relating to the use of this equipment and to file these records with the court which authorized the pen register or trap and trace. See 18 U.S.C. § 3123(a)(3).

OPR Inquiry and Civil Liability for Unauthorized Disclosures - If a court, appropriate department, or agency, 1) finds that the government violated the wiretap statute (18 U.S.C. § 2520, *et seq.*) or the Electronic Communications Privacy Act (ECPA codified at 18 U.S.C. § 2701, *et seq.*); and 2) seriously questions if a government employee acted willfully or intentionally in such violation, the statute now requires that an OPR inquiry be initiated to determine if disciplinary action is warranted. The Department of Justice Inspector General will be notified of the results of the inquiry, including justification for the outcome. Violations warranting an OPR inquiry include improper disclosure of information obtained pursuant to Title III, ECPA, a pen register/trap and trace order, and national security letters under 18 U.S.C. § 2709. The United States is now civilly liable for certain violations of FISA [Section 106(a) codified at 50 U.S.C. § 1806(a) (the use of information in the ELSUR context), Section 305(a) codified at 50 U.S.C. § 1825(a) (the use of information in the physical search context), and Section 405(a) codified at 50 U.S.C. § 1845(a) (the use of information in the pen register/trap and trace context)], the wiretap statute, and ECPA with minimum damages awarded at $10,000 plus legal fees. See 18 U.S.C. § 2520(f) & (g); 18 U.S.C. § 2707(d) & (g); and 18 U.S.C. § 2712.

Search Warrants

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

Single Jurisdiction Search Warrants for Terrorism - In domestic terrorism (as defined within the act) or international terrorism cases, a search warrant may be issued by a magistrate judge in any district in which activities related to the terrorism have occurred for a search of property or persons located within or outside of the district. See Fed. R. Crim. P. 41(a). U.S. Attorneys' Offices had been advised to coordinate all search warrants in the investigation into the September 11 terrorist attacks with the DOJ Terrorism and Violent Crimes Section in order to avoid duplication of effort and prevent inadvertent interference with ongoing investigations in another district. It is likely that DOJ will maintain some method of coordination to eliminate these concerns in other investigations as well.

Miscellaneous Tools

Obtaining Financial Records and Consumer Reports - Section 358 of the Act amended the Right to Financial Privacy Act and the Fair Credit Reporting Act to provide for the ability to obtain financial records or consumer reports related to "intelligence or counterintelligence activity, investigation or analysis related to international terrorism." See 31 U.S.C. § 5311; 12 U.S.C. § 3412(a).

DNA Predicates - Section 503 extends DNA sample collection to all federal offenders convicted of the types of offenses that are likely to be committed by terrorists (as set forth in 18 U.S.C. § 2332b(g)(5)(B)) or any crime of violence (as defined in 18 U.S.C. §16). See 42 U.S.C. §14135a(d)(2).

Emergency Assistance from DOD - The Act broadened the Attorney General's authority to request assistance from the Secretary of Defense in emergency situations involving weapons of mass destruction. See 18 U.S.C. § 2332e.

Educational Records - Law enforcement can now obtain educational records held by an educational agency or institution if they are relevant to an authorized investigation of domestic or

international terrorism or other offenses found under 18 U.S.C. § 2332b(g)(5)(B). Assistant Attorney General approval is required. This includes individually identifiable information which may be in the possession of the National Center for Education Statistics. See 20 U.S.C. § 1232g; 20 U.S.C. § 9007.

Expanded Foreign Jurisdiction - The special maritime and territorial jurisdiction of the United States explicitly is extended to U.S. diplomatic and consular premises and related private residences overseas for offenses committed by or against a U.S. national. This clarified inconsistent prior caselaw to establish that the United States may prosecute offenses committed in its missions abroad, by or against its nationals. The provision explicitly exempts offenses committed by members or employees of the U.S. armed forces and persons accompanying the armed forces, who are covered under a provision of existing law, 18 U.S.C. § 3261(a). See 18 U.S.C. § 7.

Expansion of the Computer Fraud and Abuse Act (18 U.S.C. § 1030) - The Act included a variety of modifications to strength the criminal statute used most often in computer hacking cases (18 U.S.C. § 1030). The Patriot Act increases penalties for hackers who damage protected computers (from a maximum of 10 years to a maximum of 20 years); clarifies the *mens rea* required for such offenses to make explicit that a hacker need only intend damage, not a particular *type* of damage; adds a new offense for damaging computers used for national security or criminal justice purposes; expands the coverage of the statute to include computers in foreign countries so long as there is an effect on U.S. interstate or foreign commerce; counts state convictions as "prior offenses" for the purpose of recidivist sentencing enhancements; and allows losses to several computers from a hacker's course of conduct to be aggregated for purposes of meeting the $5,000 jurisdictional threshold. See 18 U.S.C. § 1030.

II. Money Laundering

New Offenses

Bulk Cash Smuggling - The Act makes it an offense to smuggle more than $10,000 in currency into or out of the United States with the intent to evade the CMIR reporting requirement. The House Report specifically states that this provision will apply to conduct occurring before the effective date of the Act. 31 U.S.C. § 5332.

Money Transmitting Businesses - The scope of 18 U.S.C. § 1960 is expanded to include any business, licensed or unlicensed, that involves the movement of funds that the defendant knows were derived from a criminal offense, or were intended to be used "to promote or support unlawful activity." It would not be necessary for the Government to show that the business was a

storefront or other formal business open to walk-in trade. To the contrary, it would be sufficient to show that the defendant offered his services as a money transmitter to another.

It is already an offense under Sections 1956 and 1957 for any person to conduct a financial transaction involving criminally derived property. But Section 1957 has a $10,000 threshold requirement, and Section 1956 requires proof of specific intent either to promote another offense or to conceal or disguise the criminal proceeds. New Section 1960 contains neither of these requirements if the property is criminal proceeds; or alternatively, if there is proof that the purpose of the financial transaction was to commit another offense, it does not require proof that the transmitted funds were tainted by any prior misconduct. See 18 U.S.C. § 1960.

New Investigative Tools

Expansion of Money Laundering Predicates - The list of foreign crimes in the definition of "specified unlawful activity" is expanded to include public corruption and other foreign offenses. Similarly, amendment to RICO makes a long list of acts relating to terrorism predicates for money laundering. Moreover, under Section 1956(a)(2)(A), it will be an offense to send any money from any source into or out of the United States with the intent to promote such an offense.

Subpoenas for Overseas Bank Records - A new statute, 31 U.S.C. § 5318(k)(3), provides that the Attorney General or the Secretary of the Treasury may serve "a summons or subpoena" on any foreign bank that has a correspondent account in the United States, and request records relating to that correspondent account or any records maintained outside of the United States relating to the deposit of funds into the foreign bank. Congress has created this authority by requiring that any foreign bank that maintains a correspondent account in the United States must appoint a representative to accept a subpoena issued by the Attorney General or the Secretary of the Treasury for bank records. Thus, it would no longer be necessary to seek those records pursuant to a mutual legal assistance treaty or other procedure that is dependent upon the cooperation of a foreign government. This section of the Act became effective on December 25, 2001.

Long-Arm Jurisdiction - The Act expanded the court's jurisdiction to include a foreign person, including a foreign bank, if the money laundering offense occurred in part in the United States, or the foreign bank has a correspondent account in the United States. See 18 U.S.C. § 1956(b).

Voluntary Disclosure by Banks - The Act provides immunity from civil liability for any financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency. It further prohibits, with some limited exceptions, the person or entity making such disclosure from notifying the person involved in the suspicious transaction that the transaction has been reported. See 31 U.S.C. § 5318(g)(3).

III. New Terrorism Offenses

Definitions

Domestic Terrorism - The Act created a new definition of "domestic terrorism," corresponding to the existing definition of "international terrorism." The term is defined to mean activities occurring primarily within the territorial jurisdiction of the United States involving acts dangerous to human life that are a violation of the criminal laws of the United States or any state and appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by mass destruction, assassination, or kidnaping. Investigations of "domestic terrorism" and "international terrorism" have additional investigative tools including nationwide service of search warrants and disclosure of educational records. See 18 U.S.C. § 2331; Fed. R. Crim. P. 41(a); 20 U.S.C. § 1232g; 20 U.S.C. § 9007.

Federal Crime of Terrorism (18 U.S.C. § 2332b(g)(5))- The definition was modified to include several offenses likely to be committed by terrorists, including a number of aircraft violence crimes and certain computer crimes, to the list of predicate offenses. Due to Congressional concerns about overbreadth, some crimes were removed from the list (primarily offenses involving assault and less grave property crimes). These offenses are now RICO predicates (see USA Patriot Act § 813), have a longer or no statute of limitations (18 U.S.C. § 3286), and are predicates for the collection of DNA (see Section I. above).

New Offenses

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

Harboring Terrorists - Previously the harboring offense prohibited only the harboring of spies (see 18 U.S.C. §792); there was no comparable terrorism provision. The new law prohibits

harboring or concealing persons who have committed or are about to commit a variety of terrorist offenses, including destruction of aircraft or aircraft facilities, use of nuclear materials or chemical or biological weapons, use of weapons of mass destruction, arson or bombing of government property, destruction of energy facilities, sabotage of nuclear facilities, or aircraft piracy. See 18 U.S.C. § 2339.

Expert Advice/Assistance and Material Support - The prohibition on providing material support or resources to terrorists was expanded to include expert advice and assistance. This makes the offense applicable to experts who provide advice or assistance knowing or intending that it is to be used in preparing for or carrying out terrorism crimes, such as the civil engineer providing advice on the best manner to destroy a building. This provision expanded the criminal law by eliminating the restriction that such material support be within the United States, clarifying that prohibited material support includes all types of monetary instruments, and adding to the list of underlying terrorism crimes for which provision of material support is barred. Additionally, material support offenses can be prosecuted in any district in which the underlying offense was committed. The Act also clarified that the Trade Sanctions Reform and Export Enhancement Act of 2000 does not limit this prohibition. See 18 U.S.C.§ 2339A.

Possession of a Biological Agent - The Act established an additional offense to the biological weapons statute of possessing a biological agent or toxin of a type or in a quantity that, under the circumstances, is not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose. Additionally it created a new offense for certain restricted persons (including felons, persons indicted for felonies, fugitives, drug users, illegal aliens, mentally impaired persons, aliens from certain terrorist states, and persons dishonorably discharged from the U.S. armed services) to possess a biological agent or toxin listed as a "select agent" by the Secretary of Health and Human Services. See 18 U.S.C. § 175.

Attempt and Conspiracy - The Act amended several terrorism crimes to add a prohibition on attempt and conspiracy resulting in penalties equal to the underlying offenses. See 18 U.S.C. § 81 (arson); 18 U.S.C. § 930(c) (killings in federal facilities); 18 U.S.C. § 1362 (injuring or destroying communications lines or systems); 18 U.S.C. § 1363 (injuring or destroying buildings or property within the special maritime and territorial jurisdiction of the United States); 18 U.S.C. § 1992 (wrecking trains); 18 U.S.C. § 2339A (material support to terrorists); 18 U.S.C. § 2340A (torture); 42 U.S.C. § 2284 (sabotage of nuclear facilities or fuel); 49 U.S.C. § 46504 (interference with flight crew members and attendants); 49 U.S.C. § 46505 (carrying weapons aboard aircraft); and 49 U.S.C. § 60123(b) (damaging or destroying an interstate gas or hazardous liquid pipeline facility).

Additional Information and Manual Changes

Additional guidance and associated manual changes will be forthcoming. Any questions should be directed to the Investigative Law Unit, [redacted] The text of the law,

b2-1

redline/strikeout text of affected statutes and Federal Rules, and other associated documents are posted on the ILU FBI Intranet website which can be found through the OGC webpage.

LEAD (s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Distribute to all appropriate personnel.

CC: Mr. Parkinson, Rm 7427
Mr. Steele, Rm. 7159
Mr. Kelley, Rm. 7427
Ms. Gulyassy, Rm. 7159
[redacted] Rm. 7326
[redacted] Rm. 7879
[redacted] Rm. 7975
[redacted] Rm. 7975
[redacted] Rm. 7879
[redacted] Rm. 7877
ILU
Each OGC Unit Chief

b7C-1