(Rev. 01-31-2003)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

b7

Precedence: PRIORITY **Date:** 03/22/2004

To: General Counsel **Attn:** Investigative Law Unit [redacted] b6 b7C
Room 7326

From: [redacted] b2
Legal Unit
Contact: ADC [redacted] b6 b7C

Approved By: [redacted] b2

Drafted By: [redacted] b6 b7C

Case ID #: 66F-HQ-C1364260 (Pending) - 46
[redacted] (Pending) - 83390
197- [redacted] C233355 (Pending) - 4 b7A b2

Title: USA PATRIOT ACT b7E
SUNSET PROVISIONS

Synopsis: To provide [redacted] response to request for examples and summaries of use of investigative tools created by the USA PATRIOT Act. Lead covered. b2

Reference: 66F-HQ-C134260 Serial 5 b7E

Details: This EC provides a brief narrative summarizing [redacted] use of investigative tools created by the USA PATRIOT Act. A canvas was conducted of all squads in the Los Angeles Division and the following details the results:

Voice Mail - Section 209 of the Act enabled law enforcement to 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 messages on 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. See 18 U.S.C. § 2510; 18 U.S.C. § 2703.

[redacted] (S) b1 b2 b7E

~~SECRET~~

To: General Counsel Fr[redacted]: [redacted] b2
Re: 66F-HQ-C1364260, 03/22/2004 b7E

Nationwide Search Warrants for E-mail and Associated Records - Section 220 of the Act enabled courts with jurisdiction over an investigation to 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. See 18 U.S.C. § 2703.

This technique was utilized by the [redacted] following the shooting on July 4, 2002 at [redacted] International Airport. It was extremely helpful in this investigation for the Central District of California to be able to issue nationwide search warrants for information on the subject's email. b2 b7E

Voluntary Disclosures - Section 212 of the law 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. This provision also allows a communications service provider to disclose non-content records to protect their rights and property. This portion of the provision will most often be used when the communications service provider itself is a victim of computer hacking. See 18 U.S.C. § 2702(b) & (c)(3); 18 U.S.C. § 2703(c)(2)(F).

For about ten months (January 2003-November 2003) there was a mandatory reporting requirement for the receipt of content information (usually e-mail content) under this emergency disclosure provision. (See the Homeland Security Act and EC 66F-HQ-C1384970 Serial 501.) During that time, offices were only required to report the number of e-mail messages that were received under this voluntary disclosure provision. Offices were not required to report the receipt of records and were also not required to provide case information. For this reason, it would be beneficial for offices to now report more detail on these voluntary disclosures. Examples where voluntary disclosures led to valuable foreign intelligence or arrests would be particularly helpful.

[redacted] (S) Moreover, this was the practice after 9-11, where service providers voluntarily provided FBI Los Angeles with the information requested. In an emergency or crisis situation it would be imperative to the investigation for b1 b2 b7E

service providers to have this ability to voluntarily provide the FBI with this information. Where time is of the essence, giving service providers the option of revealing this information without a court order or grand jury subpoena is crucial to receiving the information quickly. This is what occurred after 9-11 and should continue to be in place in the eventuality of another such attack.

Information Sharing - Section 203(b) & (d) of the Act provided new information sharing capabilities between criminal and intelligence investigations for foreign intelligence information and information obtained via a Title III electronic surveillance. (See EC [redacted] dated 10/26/01 for additional information.) Recognizing that this tool has become a regular part of how the FBI operates, especially in terrorism cases, no statistics are necessary. However, case examples that demonstrate the importance of this tool should be provided.

b7A

All [redacted] CT and CI investigation continue to benefit from this provision of the USA PATRIOT Act. A good example of this in Los Angeles is the case where the intelligence investigation of an FBI Supervisory Special Agent and a member of the PRC revealed information that the intelligence squad was able to share with a criminal squad for prosecution on criminal charges. Information sharing has also been invaluable between CT/CI investigations and criminal investigations into violations of neutrality, fraudulent document production, passport/visa violations, immigration violations, white collar crimes, drug cases, and all types of fraud schemes.

b2
b7E

Intercepting Communications of Computer Trespassers - Section 217 of the Act clarified an ambiguity in the law by explicitly providing victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. 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 authorized users. 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). See 18 U.S.C. § 1030(e)(2); 18 U.S.C. § 2510 (20) & (21); 18 U.S.C. § 2511(2)(i).

This provision has proven especially useful to the [redacted] and is considered a key aspect of all cyber investigations. "Hackers" routinely use victim computers for SPAM and other illegal communications. Therefore, this provision has proven useful in both intelligence and criminal investigations. Recently this method has been used on at least two occasions in intelligence cases where the FBI took over the victim's on-line identity to communicate with the suspected terrorists. b2 b7E

Expanded Predicates for Title III - Sections 201 & 202 of the Act expanded the predicate offenses for Title III 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). See 18 U.S.C. § 2516. b1 b2 b7E

[redacted] (S)

yet but it is anticipated that the expanded predicate offenses for computer fraud and abuse will become essential to several Los Angeles investigations.

Roving FISA Surveillance - Section 206 amended FISA to allow the Court to issue a "generic" secondary order where the Court finds that the "actions of the target of the application may have the effect of thwarting the identification of a specified person." This means that, when a FISA target engages in trade craft designed to defeat electronic surveillance, such as by rapidly switching cell phones, Internet accounts, or meeting venues, the Court can issue an order directing "other persons," i.e., the as yet unknown cell phone carrier, Internet service provider, etc., to effect the authorized electronic surveillance. Even if the target is not engaged in obvious trade craft, we can obtain such an order as long as the target's actions may have the effect of thwarting surveillance. This allows the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order. For additional information see EC [redacted] dated 10/26/01. Any examples where roving authority has been obtained and utilized to gain valuable foreign intelligence should be provided. b7A

The roving wiretap provision has been extremely helpful in [redacted] One specific example is that Los Angeles has b2 b7E

seen counterintelligence targets change service for hard-lines, email accounts, and cell phones numerous times. The roving FISA authority has allowed for investigators to continuously monitor these targets without interruption. Changing of telephone carriers is a documented technique used by foreign intelligence officers to avoid detection. [redacted] has documented these occurrences and been able to continue coverage because of this provision. b2 b7E

New Standard for FISA Pen/Trap - Section 214 of the Act eliminated the requirement that the FISA pen/trap order include specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. FISA pen/trap and trace orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." For additional information see EC [redacted] dated 10/26/01. b7A

This provision has not proven useful to [redacted] Although the standard has been lowered the reality of the work load situation at OIPR makes this technique not viable. With the creation of the 315 classification, an agent has much better luck with getting a pen register under criminal standards than waiting for a FISA pen register to be approved. Moreover, if agents are going to take the time to fill out the paperwork for the FISA pen register, they might as well complete an actual FISA application. In one example, an agent was told she had enough for a FISA and not to waste time with the pen register. In another situation, the agent made the pen register request first and then several months later requested the FISA and never again heard anything on the pen register. If this was something that could be approved at HQ or locally, then it might be a valuable technique, but with the backlog on FISAs it is impractical to request a pen register FISA and then wait months to hear nothing. b2 b7E

Changes to "Primary Purpose" Standard for FISA - Section 218 changed FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Section 504 amended FISA to allow personnel involved in a FISA to consult with law enforcement officials in order to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such

consultation does not, in itself, undermine the required certification of "significant purpose." These changes allow FBI agents greater latitude to consult criminal investigators or prosecutors without putting their FISAs at risk. For additional information see EC 66F-HQ-A1247863 Serial 71 dated 10/26/01. While no statistics are required for this provision, case examples and brief narratives on the benefits of this provision are sought.

This is the single most important provision of the USA Patriot Act. [redacted] investigations have revealed that more often than not the suspected terrorists or intelligence officers are committing criminal violations in support of their terrorist activities. The ability to obtain a FISA order where there is substantial evidence of criminal activity and significant evidence that the proceeds are then being used to fund terrorist activities is imperative to these types of investigations. This provision also goes hand-in-hand with the information sharing provision. The shift in focus allows investigators to coordinate more with AUSAs and other law enforcement information regarding the criminal activities of terrorists. b2 b7E

New Standard for Business Records under FISA - Section 215 changed the business records authority found in Title V of FISA. The old language allowed the FISA Court to issue an order compelling the production of certain defined categories of business records upon a showing of relevance and "specific and articulable facts" giving reason to believe that the person to whom the records related was an agent of a foreign power. Section 215 changed this standard to simple relevance (just as in the FISA pen register standard described above) and gave the Court the authority to compel production of "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This is the same standard described above for Section 214. For additional information see EC [redacted] 71 dated 10/26/01. b7A

Although [redacted] views this as an extremely valuable technique [redacted] (S)

[redacted] is aware of efforts by NSLB to resolve this issue with OIPR. [redacted] would argue that this is an extremely valuable technique because of the ability to obtain records where an NSL is not appropriate. The standard of simple relevancy should be sufficient for these b1 b2 b7E

To: General Counsel From: [redacted]
Re: 66F-HQ-C1364260, 03/22/2004

investigations. NSLB should make all attempts to enforce this standard and not permit OIPR to create a higher standard which would make use of this technique more difficult. b2 b7E

[redacted] considers this lead covered.

To: General Counsel Fr[redacted]: [redacted] b2
Re: 66F-HQ-C1364260, 03/22/2004 b7E

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

Investigative Law Unit: Read and clear.

♦♦