(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

**Precedence:** ROUTINE **Date:** 03/19/2004

**To:** General Counsel ATTN: AGC [redacted] b6 b7C
Investigative Law Unit

**From:** [redacted] b2
Sqd 2
**Contact:** CDC [redacted] b7E b2

**Approved By:** [redacted] b6 b7C

**Drafted By:** [redacted]

**Case ID #:** 66F-HQ-C1364260-35 (Pending) b6 b7C

**Title:** USA PATRIOT ACT
SUNSET PROVISIONS

**Synopsis:** To provide Investigative Law Unit with examples of usage of certain sunsetted provisions of the USA Patriot Act by the [redacted]

**Details:** Per the request contained in the OGC, ILU EC dated 2/27/2004, captioned as above, the following is a synopsis of instances where certain provisions of the USA Patriot Act, subject to being sunsetted on 12/31/2005, have been utilized by [redacted] b2 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.

**305C [redacted]-42731** Nationwide search warrant for AOL. b2 b7E

On April 3, 2003, an FBI agent from [redacted] had signed onto America Online (AOL) in an undercover capacity. The agent had entered the AOL chat room [redacted] and encountered an individual using the AOL screen name [redacted] indicated that he was running a list management program in the chat room and advised that anyone wishing to join the list should type the words "list me." The Buffalo agent typed "list me" and shortly thereafter received an electronic mail (e-mail) message from [redacted] Embedded in the e-mail were nine images that depicted children engaged in sexual activity. The minors observed in these specific images had been previously identified through the FBI's Child Victim Identification Program. The agent subsequently initiated contact with [redacted] who then sent three additional e-mails to the agent. Two of the e-mails had an attached file that was a video clip of child pornography. The remaining e-mail again contained embedded images of child pornography. b6 b7C b2 b7E

Based on additional investigation [redacted] identified [redacted] as [redacted] a resident of [redacted] information was provided to [redacted] which continued the investigation of [redacted] A search warrant was eventually issued for [redacted] residence, at which time computer and other electronic evidence were seized. In an interview conducted during that search [redacted] admitted that he had engaged in the distribution and receipt of child pornography. Forensic examination of the electronic evidence supported the investigation; however, [redacted] sought to identify any additional evidence that [redacted] may have retained on AOL's server, in e-mail, etc. As such [redacted] has obtained a search warrant for [redacted] AOL account and intends to serve it during the week of March 15, 2004. It is anticipated that the warrant to be served upon AOL, located in Dulles, Virginia, will allow [redacted] to determine whether additional evidence regarding the distribution, receipt, or possession of child pornography resides in [redacted] account. In addition, [redacted] may be able to identify additional subjects, with whom [redacted] may have exchanged such images, or minors, with whom [redacted] may have been communicating.

b2
b7E
b6
b7C

[redacted] Nationwide search warrants issued as follows: b2
[redacted] to Hotmail and Verisign b7E
[redacted] to Catalog.com, Yahoo!, Hotmail, and Verisign b7A

An international group of "carders" (individuals who use and trade stolen credit card information) was operating via the Internet using Internet Relay Chat channels and various fraudulently purchased web sites. The carders needed individuals within the United States to provide "drop" sites (addresses within the country of purchase to which fraudulently purchased goods could be delivered for shipment to locations outside of that country).

Nationwide search warrants were used to obtain e-mail communications among the carders. Search warrants issued on [redacted] provided information about the fraudulent activities of the group including a drop site in [redacted] In addition, e-mail addresses for other members of the group were discovered. Nationwide search warrants were then issued on [redacted] to obtain information from the newly discovered e-mail addresses as well as updating the information from the previously known addresses.

The content produced by the e-mail providers in response to the Nationwide search warrants resulted in the indictment of the individual operating the drop site located in [redacted] The Nationwide search warrants reduced the time needed to have the searches executed and significantly reduced the number of FBI, U.S. Attorney's Office, and Judicial personnel required to complete the search warrant process. b7A

*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).

[redacted] Communications of Computer Trespasser Intercepted b2 b7E b7A

An international group of "carders" (individuals who use and trade stolen credit card information) was operating via the Internet using Internet Relay Chat channels and various fraudulently purchased web sites. The carders would use proxy servers and free e-mail accounts to conceal their identities on the Internet. Proxy servers change an Internet users origin IP address to that of the proxy server such that only the proxy server knows the true point of origin. Free e-mail accounts can be obtained without providing true identification such as names, addresses, credit card numbers, etc. One such proxy server was locate[redacted] and the [redacted] As a result, [redacted]. With b7A consent from the server's owners, all Internet traffic that passed through the proxy port was intercepted in accordance with the above Patriot Act provision.

Prior to interception, two e-mail accounts were known for the main subject. The interception led to the discovery of three additional e-mail accounts used by the main subject. The only connection between the e-mail accounts was that the subject logged onto all of the accounts around the same time on numerous occasions. One of the newly discovered e-mail accounts provided a real name and physical address information for an individual in Kuwait believed to be the main subject. The other accounts provided additional leads that would not have been possible without the interception of trespasser communications (e.g. one of the other accounts was commonly used by the main subject in additional frauds making it simpler to identify the fraud and connect them to the subject).

Any questions concerning these cases may be directed to SSA [redacted] b2
Sqd. 10 (Cyber) at [redacted] or SA [redacted] b6 b7C

To: General Counsel From: [redacted] b2
Re: 66F-HQ-C1364261 03/19/2004 b7E

**LEAD(s):**

**Set Lead 1: (Info)**

GENERAL COUNSEL

AT WASHINGTON, DC

For information and possible use by ILU in support of continuing usage of certain provisions of the USA Patriot Act beyond 12/31/2005.

◆◆