

~~SECRET~~

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE

Date: 04/21/2000

To: All Field Offices

Attn: ADIC
SAC
ASAC/CTD
CDC

From: Counterterrorism Division
International Terrorism Operations Section

Office of the General Counsel

Contact: [REDACTED]

b2
b7c

Approved By: Pickard Thomas *mp*
Gallagher Neil J. *NG*
Watson Dale L. *DLW*
Horan Sheila *SH*
Rolince Michael *MR*

b7c

[REDACTED]
Bowman Spike
[REDACTED]

Drafted By: [REDACTED] b7c

Case ID #: (S) [REDACTED] (S) b1

Title: (w) (X) Caution on FISA Issues

Synopsis: (w) (X) FBIHQ cautions all field offices on the handling of electronic surveillance and physical searches under the Foreign Intelligence Surveillance Act (FISA)

(S)(w) Classified By: ITOS/CTD
Reason: 1.5(c)
Declassify On: X1

CLASSIFIED BY: 60267 NLS/Dcm
REASON: 1.5 (C)
DECLASSIFY ON: X1
(R4D) (6/1/00)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~

~~SECRET~~

~~SECRET~~

To: All Field Offices From: Counterterrorism Division

Re: (S) [REDACTED] (S) b1

04/14/2000

Details: (u) (S) In the first quarter of the year 2000, different field offices have encountered difficulties in their management of electronic surveillances and physical searches authorized under FISA. After one quarter of reporting we are aware of potential violations numbering three and one-half times those reported in 1999. Examples of problems encountered follow:

(u) (S) In one case, a field office secured a FISA which had to be implemented by a second field office. The second field office implemented the FISA order incorrectly, and videotaped a meeting even though videotaping was not authorized in the FISA order.

(u) (S) In another investigation, a field office secured a FISA order which authorized the coverage of a target's cell phone. Unknown to the field office, some time after the FISA order, the target gave up his cell phone, and the target's cell phone number was assigned by the cell phone carrier to a new person. The new owner of the cell phone spoke a language other than the language spoken by the target of the FISA. When the language specialist listened to the FISA tape, and heard a new language, the specialist reported it to the agent working the case. Nothing was done for a substantial period of time, and timely reportedly was not made to FBIHQ. The new owner of the cell phone number was therefore the target of unauthorized electronic surveillance for a substantial period of time.

(u) (S) In a third example, a target's E-Mail was correctly intercepted under a FISA order. When time came to renew the FISA, the field office decided to omit E-Mail coverage since the coverage was not productive. Thus, the FISA renewal order did not cover E-Mail. The field office then continued to cover the target's E-Mail even though there was no authorization for E-Mail coverage in the FISA renewal order.

(u) (S) All events have been reported to the Office of Intelligence Policy and Review (OIPR) at the Department of Justice (DOJ) and to the Inspection Division, FBIHQ. OIPR, will report these incidents to Congress. If, after thorough analysis, one or more of these incidents is considered to be of sufficient gravity, the incidents will be reported to the Intelligence Oversight Board and/or to the Office of Professional Responsibility. Thus, the increase in violations of FISA court orders has the attention of the highest levels of management at the Department of Justice and the FBI.

(u) (S) Other examples include unauthorized searches, incorrect addresses, incorrect interpretation of a FISA order and overruns of ELSUR.

(u) (S) It is important that field offices read carefully every FISA package and not assume that the FISA packages are similar, have the same authorities, or, have the same rules for passing FISA material to DOJ, U.S. Attorneys offices, or even to FBI SAs working parallel criminal investigations. Every FISA

~~SECRET~~

~~SECRET~~

~~SECRET~~
~~SECRET~~
~~SECRET~~

b1
To: All Field Offices From: Counterterrorism Division

Re: ~~(S)~~ [REDACTED] (S) 04/14/2000

package must be assumed to be unique and read in its entirety by agents responsible for the investigation. All technical squads must share copies of all FISAs, and minimization procedures thereunder, with the substantive squads and CDC and vice versa. In addition, field offices should be advised that there is a 14-day reporting requirement for the field on these incidents.

(U) Any and all significant occurrences should be reported to FBIHQ to determine whether the FISA may continue, be shut down, or additional authorities sought.

(U) All CDCs have been trained in FISA and should be consulted on all FISAs. CDCs should familiarize themselves with all FISA Court orders in their field office, and advise their technical and operational squads accordingly.

(U) FBIHQ is in the process of a more in-depth review of FISA issues and will issue additional guidance to the field once that review is completed.

~~SECRET~~

~~SECRET~~