AMERICAN CIVIL LIBERTIES UNION FOUNDATION

TECHNOLOGY & LIBERTY PROGRAM

Jameel Jaffer
Staff Attorney

www.aclu.org

National Headquarters 125 Broad Street, New York, NY 10004-2400

Tel (212) 519-7814 Fax (212) 549-2629 E-mail: jjaffer@aclu.org

March 4, 2003

BY FACSIMILE: 202 616 8470

Marcia Berman
U.S. Department of Justice
Civil Division, Federal Programs, Room 7204
20 Massachusetts Ave., NW
Washington, DC 20530

Re: *ACLU et al. v. DOJ*, Civil Action No. 02-2077 (ESH)

Dear Ms. Berman,

In connection with the above-captioned case, we received yesterday from your office the Declaration of Charles M. Steele and the Second Declaration of Christine Kiefer, together with accompanying Exhibits. We have reviewed these documents and are now able to further narrow the issues to be litigated.

We do not intend to challenge the adequacy of the FBI's search. We intend to challenge the FBI's withholding of documents as indicated below.

Exhibit I

Exhibit I includes 29 pages (numbered 1-29) released to us by letter dated February 21, 2003. It is our understanding that Exhibit I also includes 50 pages (numbered 30-79) that have not been released to us.

With respect to Exhibit I, we will challenge the invocation of Exemption (b)(1) on pages 1-5. We will not challenge any Exemption relied on in pages 6-29. We will challenge all Exemptions relied on in pages 30-79, except (i) we will not challenge any invocation of Exemption (b)(2)-1 or (b)(7)(C)-1; and (ii) we will not challenge the invocation of Exemption (b)(1) on pages 31, 33, 37, 39, 40-41, 42-43, 45, 46, 47, 49, 51, 52, 53, 54, 55, 56, 58-59, 68, 70, 71, 72, 73, 75, 76, and 79. In waiving our right to challenge the FBI's reliance on Exemptions (b)(2)-1 and (b)(7)(C)-1, we are of course assuming that the material excised pursuant to these Exemptions consists solely of telephone and pager numbers or of names and identifying information of FBI employees. *See* Second Declaration of Christine Kiefer, at p. 8.

Exhibit A
Civil Action No. 02-2077(ESH)

Exhibit II

Exhibit II consists of 24 pages released by letter dated November 14, 2002; 14 pages released by letter dated January 16, 2003; and 41 pages released by letter dated January 31, 2003.

We will not challenge any Exemption relied on in Exhibit II, except (i) we will challenge the FBI's reliance on Exemption (b)(5) on pages 36 and 37; (ii) we will challenge its reliance on Exemption (b)(1) on pages 38-43; and (iii) we will challenge all Exemptions relied on in pages 54-57 and 71-74.

Exhibit III

Exhibit III consists of 1 page released on March 3, 2003. The FBI has not relied on any Exemption with respect to this document.

Please feel free to contact me if you have questions about this letter.

Sincerely,

Jameel Jaffer

cc: David Sobel

EXHIBIT I

Documents released by letter dated February 21, 2003

U.S. Department of Justice

Federal Bureau of Investigation
935 Pennsylvania Ave., N.W.

Washington, D.C. 20535-0001

FEB 21 2003

Ms. Ann Beeson
American Civil Liberties Union Foundation
125 Broad Street
New York, New York 10004-2400

Subject of Request: DOJ RESPONSE TO 6/13/02 LETTER FROM CONGRESSMEN

FOIPA No. 966750-1 /190- ____________

Dear Requester:

Enclosed are copies of documents from FBI records. Excisions have been made to protect information exempt from disclosure pursuant to Title 5, United States Code, Section 552 (Freedom of Information Act) and/or Section 552a (Privacy Act). In addition, where excisions were made, the appropriate exempting subsections have been cited opposite the deletions. Where pages have been withheld in their entirety, a deleted page information sheet has been substituted showing the reasons or basis for the deletion. The subsections cited for withholding information from the enclosed documents are marked below:

Section 552		Section 552a
☒ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☒ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3) ____________	☒ (b)(7)(C)	☐ (k)(1)
____________	☐ (b)(7)(D)	☐ (k)(2)
____________	☐ (b)(7)(E)	☐ (k)(3)
____________	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☒ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

(See Form OPCA-16a, enclosed, for an explanation of these exemptions.)

Pursuant to your request, 79 pages(s) were reviewed and 29 page(s) are being released.

During the review of material pertinent to the subject of your request, documents were located which

☐ originated with another Government agency(ies).
These documents were referred to that agency(ies) for review and direct response to you.

☐ contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

1 - EPIC - Attention: David Sobel, Esquire

☒ If you desire, you may appeal any denials contained herein. Appeals should be directed in writing to the Co-Director, Office of Information and Privacy, U.S. Department of Justice, Flag Building, Suite 570, Washington, D.C. 20530-0001 within sixty days from receipt of this letter. The envelope and the letter should be clearly marked "Freedom of Information Appeal" or "Information Appeal." Please cite the FOIPA number assigned to your request so that it may be easily identified.

☐ The enclosed material is from the main investigative file(s) in which the subject of your request was the subject of the investigation. There are additional references to the subject(s) of your request in files relating to other individuals, organizations, events or activities. These additional mentions or references have not been reviewed to determine if, in fact, they are identifiable with the subject(s) of your request. Our experience has shown that such references are frequently similar to information contained in the processed main file(s). We will process these references if you now make a specific request for them. However, because of a significant increase in FOIPA requests and an expanding backlog, we have given priority to the processing of main investigative files and can only complete the processing of these additional references as time and resources permit.

☐ See additional information which follows.

Sincerely yours,

Chief
Freedom of Information-
Privacy Acts Section
Records Management Division

Enclosures (2)

~~SECRET~~ FISA

[redacted] (S) b1

2/4/2003

b1 (S) [redacted]

[redacted]

S b1

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

FEB 5 2003 AUC 63633

CLASSIFIED BY: ckkh

REASON: 1.5 (c)

DECLASSIFY ON: X 1

CA # 02-CV-2077

~~SECRET~~

CLASSIFIED DECISIONS FINALIZED BY DEPARTMENT REVIEW COMMITTEE (DRC) DATE: FEB 13 2003 AUC 63633 ckkh

SECRET

Page 7

[redacted]

(S)

SECRET

FISA

2/4/2003

Pen Registers since 10/26/2001

ALL INFORMATION CONTAINED
HERE IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

ProjectNumber	CompletedDate
[redacted]	

(S) b1

CLASSIFIED DECISIONS FINALIZED
BY DEPARTMENT REVIEW COMMITTEE (DRC)
DATE: FEB 1 3 2003 62033 CK/KH
Civil Action # 02-cv-2077

FEB 5 2003 AUC 62033
CLASSIFIED BY: CK KH
REASON: 1.5 (c)
DECLASSIFY ON: X 1
CA # 02-CV-2077

SECRET

3

~~SECRET~~

ProjectNumber	CompletedDate
[redacted]	

(S)

b1

b1

Grand Total: [redacted] (S)

~~SECRET~~

4

~~SECRET~~

Business Record Order Requests Since 10/26/2001

ALL INFORMATION CONTAINED
HERE IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

ProjID	DateReceived
[redacted]	

(S) b1

Grand Total: [redacted] (S) b1

FEB 10 2003 Aug 6 2033
CLASSIFIED BY: ck/ck
REASON: 1.5 (C)
DECLASSIFY ON: X 1
Civil Action # 02-cv-2077

CLASSIFIED DECISIONS FINALIZED
BY DEPARTMENT REVIEW COMMITTEE (DRC)
DATE: FEB 13 2003 Aug 6 2033 ck
Civil Action # 02-cv-2077

~~SECRET~~

5

SECRET

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE **Date:** 10/26/2001

To: All Divisions **Attn:** ADIC, SAC
CDC

From: Office of the General Counsel
NSLU/NSLB, Room 7975
Contact: National Security Law Unit, [redacted] b2-1

Approved By: Mueller Robert S III
Pickard Thomas J
Parkinson Larry R
Bowman M E
[redacted] b7C-1

Drafted By: [redacted]mjw b7C-1

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

Case ID #: 66F-HQ-A1247863 (None)

Title: NEW LEGISLATION
REVISIONS TO FCI/IT LEGAL AUTHORITIES
NATIONAL SECURITY LETTERS

Synopsis: Summarizes recent changes to FCI/IT legal authorities relating to NSLs, and describes implementation procedures.

Details:

Background

On October 26, 2001, the President signed the "Uniting and Strengthening America Act" which significantly revises many national security legal authorities. In particular, the Act changes key features of existing National Security Letter (NSL) authority. This communication summarizes the changes to NSL authorities; related serials describe other changes effected by the Act. A separate EC of this same date addresses various other FISA-related provisions of the Act.

NSL are issued in FCI/IT investigations to obtain telephone and electronic communications records from telephone companies and Internet Service Providers (pursuant to the Electronic Communications Privacy Act, or ECPA), records from financial institutions (pursuant to the Right to Financial Privacy Act), and information from credit bureaus (pursuant to the Fair Credit Reporting Act). Delay in obtaining NSLs has long been identified as a significant problem in FCI/IT investigations. Two factors have contributed most prominently to

DECLASSIFIED BY [illegible] ON FEB 13 2003
Civil Action # 02-CV-2077

FEB 4 2003
CLASSIFIED BY: [illegible]
REASON: 1.5 (c)
DECLASSIFY ON: X 1
CA# 02-CV-2077

SECRET

b

this delay: the complexity of the standard predication for NSLs and the requirement that signature authority be restricted to officials no lower than Deputy Assistant Director. Intending to streamline the investigative process, the new Act addresses both of these issues. Section 505 of the Act changes the standard predication for all three types of NSLs to simple relevance and allows the Director to delegate signature authority to SACs.

New Standard Predication

Under the new law, all three NSLs are now available when the signature authority certifies that the information sought is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States." Prior to the Act, the statutes required both relevance and "specific and articulable facts" giving reason to believe that the subject is an agent of a foreign power (or, in the case of subscriber requests, had been in contact with such an agent). This "agent of a foreign power" prong of the standard made it necessary to collect and document specific facts demonstrating that the standard had been met. This requirement and the complexity of the standard itself often led to extensive delays in generating NSLs. The new law makes the NSL standard roughly analogous to that for a criminal subpoena.

This new standard requires that the information sought be relevant to an "ongoing investigation to protect against international terrorism or clandestine intelligence activities." [Use of this technique is authorized in full investigations properly opened under the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations ("FCI AGG"). The technique also may be authorized in preliminary inquiries, with prior coordination through the relevant NSD or CTD unit at FBIHQ.] Although the language differs somewhat from that used in the previous versions of the statute, OGC and DOJ take the position that all investigations authorized pursuant to the FCI AGG are "to protect against international terrorism or clandestine intelligence activities." (S)(4)

The Act also inserts the language "provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States." Congress inserted this to indicate that the techniques will not be used against U.S. persons who are merely exercising constitutionally protected rights. However, it is highly unlikely, if not entirely impossible, for an investigation to be authorized under the FCI AGG that is "solely" based on protected activities. In other words, all authorized investigations of U.S. persons will likely involve some allegation or possibility of illegal activity (e.g., terrorism, espionage, clandestine intelligence activities, etc.) which is not protected by the First Amendment.

Finally, the new standard does not mean that NSLs are available only on the <u>subjects</u> of investigations. An NSL is available when the information sought is "relevant" to the investigation, as described above. For example, information concerning apparent associates of, or individuals in contact with, the subject of a investigation, may be relevant.

<u>Signature Authority</u>

The Act allows the Director to delegate signature authority down to Deputy Assistant Directors at FBIHQ and SACs in "designated" field offices. The current statute allows only for delegation to DADs. Thus, NSL authority now is delegated to only the ADs and DADs in NSD and CTD, and to the ADICs at LA, NY, and WFO.

The new legislation allows delegation to the SACs in field offices "designated by the Director." This language reflects Congress' intention that the delegation not occur automatically, but that the Director choose which offices needed, and were properly prepared to exercise, delegated authority. The Director soon will make initial delegations to field offices in a separate communication. Field offices with delegated authority will receive detailed instructions on the process of preparing and issuing NSLs. **SACs should not sign NSLs until they have been properly designated by the Director.** Offices not receiving delegated authority should continue to submit NSL requests through the relevant units in NSD and CTD at FBIHQ. NSLU will continue to prepare these letters.

<u>Changes in Statutory Language</u>

What follows are the actual changes in the three statutes governing NSLs. A "redlined" version showing additions and deletions is given first. A clear copy of the new version then follows.

1. **Electronic Communications Privacy Act (ECPA)**

U.S.C. § 2709: (S. 1510 Sec. 506)

SECRET

To: All Divisi From: Office of the Gene. l Counsel
Re: 66F-HQ-A1247863, 10/26/2001

"Redlined" Text Key: New text ~~Removed text~~

§ 2709. Counterintelligence access to telephone toll and transactional records

(a) Duty to provide.--A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required certification.--The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may--

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee ~~in a position not lower than Deputy Assistant Director~~) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment of the Constitution of the United States; and ~~made that--~~

~~(A) the name, address, length of service, and toll billing records sought are relevant to an authorized foreign counterintelligence investigation; and~~

~~(B) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801); and~~

SECRET

9

(2) request the name, address, and length of service of a person or entity if the Director (or his designee ~~in a position not lower than Deputy Assistant Director~~) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States ~~made that--~~

~~(A) the information sought is relevant to an authorized foreign counterintelligence investigation; and~~

~~(B) there are specific and articulable facts giving reason to believe that communication facilities registered in the name of the person or entity have been used, through the services of such provider, in communication with--~~

~~(i) an individual who is engaging or has engaged in international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States; or~~

~~(ii) a foreign power or an agent of a foreign power under circumstances giving reason to believe that the communication concerned international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States.~~

(Remainder of statute unchanged)

New Version of 18 U.S.C. § 2709 (without redlining)

§ 2709. Counterintelligence access to telephone toll and transactional records

(a) Duty to provide.--A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required certification.--The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may--

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States; and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States.

(Remainder unchanged)

2. **Right to Financial Privacy Act**

"Redlined" version of 12 U.S.C. § 3414(a)(5)

//

(5)(A) Financial institutions, and officers, employees, and agents thereof, shall comply with a request for a customer's or entity's financial records made pursuant to this subsection by the Federal Bureau of Investigation when the Director of the Federal Bureau of Investigation (or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director) certifies in writing to the financial institution that such records are sought for foreign counterintelligence purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States. ~~sought for foreign counterintelligence purposes and that there are specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign power or an agent of a foreign power as defined in section 1801 of Title 50.~~

(Remainder unchanged)

New version of 12 U.S.C. § 3414(a)(5)

(5)(A) Financial institutions, and officers, employees, and agents thereof, shall comply with a request for a customer's or entity's financial records made pursuant to this subsection by the Federal Bureau of Investigation when the Director of the Federal Bureau of Investigation (or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director) certifies in writing to the financial institution that such records are sought for foreign counterintelligence purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States.

(Remainder unchanged)

3. **Fair Credit Reporting Act**

"Redlined" Version of 15 U.S.C. § 1681u

§ 1681u. Disclosures to FBI for counterintelligence purposes

(a) Identity of financial institutions

Notwithstanding section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish to the Federal Bureau of Investigation the names and addresses of all financial institutions (as that term is defined in section 3401 of Title 12) at which a consumer maintains or has maintained an account, to the extent that information is in the files of the agency, when presented with a written request for that information, signed by the Director of the Federal Bureau of Investigation, or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, which certifies compliance with this section. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing, that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States ~~in writing that—~~

~~(1) such information is necessary for the conduct of an authorized foreign counterintelligence investigation; and~~

~~(2) there are specific and articulable facts giving reason to believe that the consumer—~~

~~(A) is a foreign power (as defined in section 1801 of Title 50) or a person who is not a United States person (as defined in such section 1801 of title 50) and is an official of a foreign power; or~~

~~(B) is an agent of a foreign power and is engaging or has engaged in an act of international terrorism (as that term is defined in section 1801(c) of Title 50) or clandestine intelligence activities that involve or may involve a violation of criminal statutes of the United States.~~

(b) Identifying information

Notwithstanding the provisions of section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request, signed by the Director or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States. ~~in writing that~~

~~(1) such information is necessary to the conduct of an authorized counterintelligence investigation; and~~

~~(2) there is information giving reason to believe that the consumer has been, or is about to be, in contact with a foreign power or an agent of a foreign power (as defined in section 1801 of Title 50).~~

(c) Court order for disclosure of consumer reports

Notwithstanding section 1681b of this title or any other provision of this subchapter, if requested in writing by the Director of the Federal Bureau of Investigation, or a designee of the Director in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, a court may issue an order ex parte directing a consumer reporting agency to furnish a consumer report to the Federal Bureau of Investigation, upon a showing in camera that the report is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States. ~~in camera that—~~

~~(1) the consumer report is necessary for the conduct of an authorized foreign counterintelligence investigation; and~~

~~(2) there are specific and articulable facts giving reason to believe that the consumer whose consumer report is sought—~~

~~(A) is an agent of a foreign power, and~~

~~(B) is engaging or has engaged in an act of international terrorism (as that term is defined in section 1801(c) of Title 50) or clandestine intelligence activities that involve or may involve a violation of criminal statutes of the United States.~~

The terms of an order issued under this subsection shall not disclose that the order is issued for purposes of a counterintelligence investigation.

(Remainder unchanged)

New Version of 15 U.S.C. § 1681(u)

§ 1681u. Disclosures to FBI for counterintelligence purposes

(a) Identity of financial institutions

Notwithstanding section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish to the Federal Bureau of Investigation the names and addresses of all financial institutions (as that term is defined in section 3401 of Title 12) at which a consumer maintains or has maintained an account, to the extent that information is in the files of the agency, when presented with a written request for that information, signed by the Director of the Federal Bureau of Investigation, or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, which certifies compliance with this section. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing, that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States.

(b) Identifying information

Notwithstanding the provisions of section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request, signed by the Director or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States.

(c) Court order for disclosure of consumer reports

> Notwithstanding section 1681b of this title or any other provision of this subchapter, if requested in writing by the Director of the Federal Bureau of Investigation, or a designee of the Director in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, a court may issue an order ex parte directing a consumer reporting agency to furnish a consumer report to the Federal Bureau of Investigation, upon a showing in camera that the report is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States. The terms of an order issued under this subsection shall not disclose that the order is issued for purposes of a counterintelligence investigation.
>
> (Remainder unchanged)

<u>Questions and Additional Information</u>

The National Security Law Unit (202-324-3951) is available to answer questions about this legislation. In addition, materials relating to the new legislation will be posted on the NSLU FBI Intranet website, which can be found <u>http://30.100.99.18/ogc/nslu/</u> or through the OGC page.

SECRET

LEAD(s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Disseminate to personnel involved in FCI/IT operations and to other division personnel as appropriate.

♦♦

SECRET

18

(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 62033 EK/JS

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

<u>New Offenses</u>

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.

<u>New Investigative Tools</u>

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. osted

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).

<u>Additional Information and Manual Changes</u>

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

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

50 Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☒ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		**Section 552a**
☒ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☒ (b)(2) - 1, 2	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☒ (b)(7)(C) - 1	☐ (k)(1)
______	☐ (b)(7)(D)	☐ (k)(2)
______	☐ (b)(7)(E)	☐ (k)(3)
______	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☒ (b)(5) - 1	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

______ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

______ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

______ Pages were not considered for release as they are duplicative of ______

______ Page(s) withheld for the following reason(s): ______

☐ The following number is to be used for reference regarding these pages:

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

30 - 79

FBI/DOJ

EXHIBIT II

Documents released by letter dated November 14, 2002

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

November 14, 2002

MS ANN BEESON
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 BROAD STREET
NEW YORK, NY 10004 2400

Subject: ALL RECORDS RE: DOJ RESPONSE TO 6/13/02, LETTER FROM CONGRESSMEN SENSENBRENNER

FOIPA No. 0966750- 000

Dear Requester:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Deletions have been made to protect information which is exempt from disclosure, with the appropriate exemptions noted on the page next to the excision. In addition, a deleted page information sheet was inserted in the file to indicate where pages were withheld entirely. The exemptions used to withhold information are marked below and explained on the enclosed Form OPCA-16a:

Section 552		Section 552a
☐(b)(1)	☐(b)(7)(A)	☐(d)(5)
☐(b)(2)	☐(b)(7)(B)	☐(j)(2)
☐(b)(3)__________	☒(b)(7)(C)	☐(k)(1)
__________	☐(b)(7)(D)	☐(k)(2)
__________	☐(b)(7)(E)	☐(k)(3)
__________	☐(b)(7)(F)	☐(k)(4)
☐(b)(4)	☐(b)(8)	☐(k)(5)
☐(b)(5)	☐(b)(9)	☐(k)(6)
☐(b)(6)		☐(k)(7)

24 **page(s)** were reviewed and 24 **page(s)** are being released.

☐ Document(s) were located which originated with, or contained information concerning other Government agency(ies) [OGA]. This information has been:

- ☐ referred to the OGA for review and direct response to you.
- ☐ referred to the OGA for consultation. The FBI will correspond with you regarding this information when the consultation is finished.

☒ You have the right to appeal any denials in this release. Appeals should be directed in writing to the Co-Director, Office of Information and Privacy, U.S. Department of Justice, Flag Building, Suite 570, Washington, D.C. 20530-0001 within sixty days from receipt of this letter. The envelope and the letter should be clearly marked "Freedom of Information Appeal" or "Information Appeal." Please cite the FOIPA number assigned to your request so that it may be easily identified.

☐ The enclosed material is from the main investigative file(s) in which the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown, when ident, references usually contain information similar to the information processed in the main file(s). Because of our significant backlog, we have given priority to processing only the main investigative file(s). If you want the references, you must submit a separate request for them in writing, and they will be reviewed at a later date, as time and resources permit.

☐ See additional information which follows.

Sincerely yours,

David M. Hardy
Section Chief,
Records Information
and Dissemination Section
Records Management Division

Enclosure(s) (2)

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE Date: 10/26/2001

To: All Divisions Attn: ADIC, SAC
CDC

From: Office of the General Counsel
NSLU/NSLB, Room 7975
Contact: National Security Law Unit, [redacted] b2-1

Approved By: Mueller Robert S III
Pickard Thomas J
Parkinson Larry R
Bowman M E
[redacted] b7C-1 b7C

Drafted By: [redacted]:mjw

Case ID #: 66F-HQ-A1247863 (None)

Title: NEW LEGISLATION
REVISIONS TO FCI/IT LEGAL AUTHORITIES
FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

Synopsis: Summarizes recent changes to FISA statute and related legal authorities.

Details:

Background

On October 26, 2001, the President signed the "Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" which significantly revises many legal authorities relating to counterterrorism. The Act, which consists of more than 150 sections, effects changes in national security authorities, the substantive criminal law, immigration law, money laundering statutes, victim assistance statutes, and other areas. The National Security Law Unit, OGC, is issuing guidance on those portions of the Act relating to national security operations. This communication addresses changes in the Foreign Intelligence Surveillance Act of 1978 (FISA) and certain other statutes relating to information sharing; a related serial describes changes to National Security Letter authorities. Other OGC communications address the non-national security law portions of the Act.

11-6-02
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-6-02 BY 60267 NLS/EP/CT
#966750

In the wake of the September 11, 2001 attacks, the Administration proposed to Congress a variety of proposals to increase the efficiency and effectiveness of FCI/IT operations, and a substantial portion of the Act is given over to this purpose. In particular, the Act seeks to improve the efficiency of the FISA process and to remove barriers to the timely sharing of information between FCI/IT intelligence operations and criminal investigations.

Many provisions of the Act, including most of the national security provisions, are subject to the "sunset" provision described in Section 224 of the Act. This Section states that the authorities expire on December 31, 2005. At that time, Congress will have to decide whether or not to re-authorize the provisions.

The following summarizes the changes in national security authorities by various sections in the Act (A separate EC of this same date addresses changes to National Security Letter (NSL) authorities). For each section, there is a summary of potential changes in FBI operational procedures. Recipients should note that this is only initial guidance; more detailed explanations and procedures may follow in subsequent communications.

1. Sharing Grand Jury, Title III and Criminal Investigative Information

Section 203 first amends Federal Rule of Criminal Procedure 6(e) to permit the disclosure of grand jury information involving intelligence information "to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties." The Section also requires subsequent notice to the Court of the agencies to which information was disseminated and adds a definition of "foreign intelligence information" to Rule 6(e). The Grand Jury portion of this Section (Section 203(a)) is not subject to the sunset provision.

Section 203 then amends Title III to allow the same sort of disclosure of Title III information when the matters involve foreign intelligence "to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties." The Section adds a definition of foreign intelligence information to Title III, and requires the Attorney

General to develop procedures for the sharing of Grand Jury or Title III information that identifies a U.S. person.

Finally, Section 203 establishes that "notwithstanding any other law" it is lawful for criminal investigators to share foreign intelligence information obtained in the course of a criminal investigation with any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official, as above.

The intent of Section 203 is to eliminate barriers to the timely sharing of information between criminal investigators and other entities (the Intelligence Community, the INS, DoD, etc.) involved in the protection of the national security. The Section essentially gives the FBI full discretion to share criminal investigative information, regardless of its source, whenever it involves foreign intelligence information (which is defined to include all foreign intelligence, counterintelligence, and counterterrorism information).

Procedural Changes: FBI components in possession of information obtained through criminal investigative techniques that is also foreign intelligence information should arrange for the appropriate dissemination of the information. Dissemination to the Intelligence Community must be coordinated through the relevant NSD or CTD units at FBIHQ. When the DOJ issues procedures relating to the dissemination of U.S. person information, the field will receive additional guidance.

2. "Roving" FISA ELSUR Authority

Section 206 amends 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 tradecraft designed to defeat ELSUR, 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 tradecraft, we can obtain such an order as long as the target's actions may have the effect of thwarting surveillance. This will allow 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. It is likely that the Court will require certain procedures for the use of this authority, to include special minimization requirements and timely after-the fact reporting.

Procedural Changes: When the field wants to obtain roving ELSUR authority, the request for a FISA sent to FBIHQ should include specific facts that will allow the Court to find that the actions of the target may have the effect of thwarting the requested surveillance, absent the roving authority. Such facts could include examples of previous tradecraft by the target, by members of the target's group or service, or by others with training or background similar to that presumed for the target. DOJ/OIPR may issue more detailed guidance as experience with this provision grows.

3. Changes in the Duration of FISA Authority

Section 207 extends the standard duration for several categories of FISA orders. First, the section allow for ELSUR and search orders on non-U.S. person agents of a foreign power pled under Section 101(b)(1)(A) of FISA (i.e., officers and employees of foreign powers, including members of international terrorist groups) to run for an initial period of 120 days (instead of 90) and to be renewed for periods of one year. The section also extends the standard duration of physical search orders in all other cases (U.S. persons and non-officer/employee targets) from 45 to 90 days.

Procedural Changes: None are required. OIPR will transition existing coverages to the new durations as they come up for renewal.

4. Expansion of the FISA Court

In order to increase the availability of FISA judges, Section 207 expands the Court from seven judges to eleven judges, three of whom must reside in the Washington, D.C. area.

Procedural Changes: None are required.

5. Changes in FISA Pen Register/Trap and Trace Authority

Section 214 makes a substantial revision to the standard for a FISA pen register/trap and trace. Prior to the Act, FISA pen registers required two showings: (1) relevance to an investigation, and (2) 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. Section 214 simply eliminates the second of the required showings. 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 <u>relevant to an ongoing investigation</u> 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 new standard requires that the information sought be relevant to an "ongoing investigation to protect against international terrorism or clandestine intelligence activities." Use of this technique is authorized in full investigations properly opened under the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations ("FCI AGG"). The technique also may be authorized in preliminary inquiries, with prior coordination through the relevant NSD or CTD unit at FBIHQ. Although the language differs somewhat from that used in the previous versions of the statute, OGC and DOJ take the position that all investigations authorized pursuant to the FCI AGG are "to protect against international terrorism or clandestine intelligence activities."

The Section also inserts the language "provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States." Congress inserted this to indicate that the technique will not be used against U.S. persons who are merely exercising constitutionally protected rights. However, it is highly unlikely, if not entirely impossible, for an investigation to be authorized under the FCI AGG that is "solely" based on protected activities. In other words, all authorized investigations of U.S. persons will likely involve some allegation or possibility of illegal activity (e.g., terrorism, espionage, clandestine intelligence activities, etc.) which is not protected by the First Amendment.

Finally, the new standard does not mean that FISA pen register/trap and trace authority is only available on the <u>subjects</u> of investigations. The authority is available when the information sought is "relevant" to the investigation, as described above. For example, information concerning apparent associates or, or individuals in contact with, the subject of a investigation, may be relevant.

<u>Procedural Changes</u>: None are required. The field may continue to request FISA pen register/trap and trace authority through FBIHQ in the established manner. However, the requests now need only contain a brief statement explaining the nature of the investigation and the relevance to that investigation of the information sought through the pen register. NSLU and OIPR will

develop additional guidance streamlining the process for requesting this authority.

6. Changes in FISA Business Records Authority

Section 215 changes 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 (the records of common carriers, public accommodations, vehicle rentals, and storage facilities) 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 changes this standard to simple relevance (just as in the FISA pen register standard described above) and gives 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.

In the past, the FBI has encountered situations in which the holders of relevant records refused to produce them absent a subpoena or other compelling authority. When those records did not fit within the defined categories for National Security Letters or the four categories then defined in the FISA business records section, the FBI had no means of compelling production. With the new language the FBI can seek a FISA court order for any such materials.

Procedural Changes: None are required. The field may continue to request business records orders through FBIHQ in the established manner. However, such requests may now seek production of any relevant information, and need only contain information establishing such relevance. NSLU and OIPR will develop additional guidance streamlining the process for requesting this authority.

7. Changes to "Primary Purpose" Standard in FISA

Sections 218 and 504 clarify the "primary purpose" issue in the FISA statute. In its prior form, the FISA required a certification that foreign intelligence be "the" purpose of the requested authority. The FISA Court interpreted this to mean that foreign intelligence, as opposed to criminal prosecution, had to be the "primary" purpose of the requested authority. Thus, interaction between FBI personnel involved in a FISA and criminal prosecutors could call into question the primary intelligence purpose of the FISA (by indicating a purpose different from foreign intelligence). As a result, FISA pleadings have often contained detailed accounts of all communication with criminal prosecutors in cases involving FISA.

Section 218 changes FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Section 504 amends FISA to allow that personnel involved in a FISA may consult with law enforcement officials 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 are meant to allow FBI agents greater latitude to consult criminal investigators or prosecutors without putting their FISAs at risk. As such, these changes address extraordinarily complex issues that have long occupied the FISA Court and DOJ. FBIHQ expects that DOJ shortly will issue revised policy on these topics.

Procedural Changes: None are required at present. The field should be aware that greater consultation with prosecutors is now possible, but, given the continuing uncertainty surrounding these issues, should continue to coordinate such consultation through FBIHQ. Additional guidance will be issued.

8. Civil Liability for Unauthorized Disclosure

Section 223 establishes civil liability for certain unauthorized disclosures, including unauthorized disclosures of FISA information. In reference to FISA, this is simply an expansion of existing civil liability, and should not significantly affect operations (since unauthorized disclosure of FISA information is already subject to more severe criminal penalties).

Procedural Changes: None are required. OGC may issue a more detailed analysis of this provision at a later date.

9. Immunity for Compliance with FISA

Section 225 grants providers of wire or electronic communication service, landlords, custodians, and other persons with immunity from civil liability for complying with the requirements of FISA. This provision simply clarifies that persons assisting the FBI in the execution of a FISA order are not at risk of civil lawsuits.

Procedural Changes: None are required.

10. **Disclosure of Foreign Intelligence Information to the DCI**

Section 905 establishes an affirmative requirement, subject to certain exceptions, that federal law enforcement components must expeditiously disclose to the Director of Central Intelligence any foreign intelligence acquired in the course of criminal investigations. The Attorney General will, within the next six months, develop guidelines to govern such disclosures.

Procedural Changes: Disclosures of foreign intelligence to the DCI should occur through FBIHQ, using established liaison channels. Field offices with previously undisseminated foreign intelligence in criminal investigations should communicate the information to FBIHQ. Additional guidance will be issued once the Attorney General has promulgated the required procedures.

11. **Computer Trespass Amendment to FISA**

Section 1003 incorporates into FISA a definition of "computer trespass" established for the criminal law in another section of the Act. The computer trespass language basically allows that an unauthorized intruder into a computer system (e.g., a hacker) can be subjected to surveillance with the consent of the owner of the computer system and without additional legal authority (before this change, we typically would have had to seek a Title III in criminal investigations). Section 1003 is a technical amendment clarifying that this language applies to the FISA as well. Therefore, under the same conditions as are established in the criminal law, FISA ELSUR authority will not be needed to conduct surveillance of a computer intruder.

Procedural Changes: Offices that believe this new language applies to an investigation should bring the matter to the attention of FBIHQ and seek a legal opinion from NSLU.

Questions and Additional Information

The National Security Law Unit [redacted] is available to answer questions about this legislation. In addition, materials relating to the new legislation will be posted on the NSLU FBI Intranet website, which can be found

b2-1

http://30.100.99.18/ogc/nslu/ or through the OGC Home Page.

LEAD(s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Disseminate to personnel involved in FCI/IT operations and to other division personnel as appropriate.

◆◆

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE **Date:** 11/28/2001

To: All Field Offices **Attn:** ADIC;
SAC;
CDC
FCI/IT Supervisors

Counterterrorism AD Watson;
DADs;
Section Chiefs

National Security AD Gallagher;
DADs;
Section Chiefs

From: General Counsel
National Security Law Unit, Room 7975
Contact: [redacted] b2-1

Approved By: Mueller Robert S III
Pickard Thomas J
Parkinson Larry R
Bowman M E

b7C

Drafted By: [redacted] mjw
R Jr:jrl

b7C-1

Case ID #: 66F-HQ-A1255972

Title: NATIONAL SECURITY LETTER MATTERS

Synopsis: Provides guidance on the preparation, approval, and service of National Security Letters (NSLs).

Reference: 66F-HQ-A1255972 Serial 15

Enclosure(s):
1) Subscriber Information NSL Model
2) Toll Billing Records NSL Model
3) Electronic Subscriber Information NSL Model
4) Electronic Communication Transactional Records NSL Model
5) Financial Records NSL Model
6) Identity of Financial Institutions NSL Model
7) Consumer Identifying Information NSL Model
8) Subscriber/Electronic Subscriber (EC) Model
9) Toll/Transactional Records EC Model
10) Financial Records EC Model
11) Financial Institutions/Consumer Identity EC Model
12) ECPA NSL Checklist
13) RFPA NSL Checklist

11-6-02
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-6-02 BY 60267 NLS/EP/CLT
#966950

11

14) FCRA NSL Checklist

Details: In the referenced communication, dated 11/09/2001, the Director of the FBI delegated the authority to certify NSLs to the following officials: (1) the Deputy Director; (2) The Assistant Directors (ADs) and all Deputy Assistant Directors (DADs) of the Counterterrorism Division (CTD) and the National Security Division (NSD); (3) the General Counsel and the Deputy General Counsel for National Security Affairs (DGC), Office of the General Counsel (OGC); (4) the Assistant Director in Charge (ADIC), and all Special Agents in Charge (SACs), of the New York, Washington, D.C., and Los Angeles field divisions; and (5) the SACs in all other field divisions. The purpose of this electronic communication is to provide comprehensive guidance on the preparation, approval, and service of NSLs.

I. <u>Introduction to National Security Letters</u>

NSLs are administrative subpoenas that can be used to obtain several types of records. There are three types of NSLs. First, pursuant to the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709, the FBI can issue NSLs for: (1) telephone subscriber information (limited to name, address, and length of service); (2) telephone local and long distance toll billing records; and (3) electronic communication transactional records. Second, pursuant to the Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3414(a)(5), the FBI can issue NSLs to obtain financial records from banks and other financial institutions. Finally, pursuant to the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681u, the FBI can issue NSLs to obtain consumer identifying information and the identity of financial institutions from credit bureaus.

NSLs are tools available in investigations conducted under the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG). The FCIG currently provide that an NSL can be issued during the course of a full international terrorism or foreign counterintelligence investigation. **NSLs cannot be used in criminal investigations unrelated to international terrorism or clandestine intelligence activities.** Given the new statutory language, the OGC and DOJ have taken the position that NSLs also may be authorized in foreign counterintelligence (FCI) and international terrorism (IT) preliminary inquiries (PIs), with prior coordination through the relevant NSD or CTD unit at FBIHQ. This position is based on the conclusion that all investigations authorized under the FCIG, including PIs, are to "protect against international terrorism or clandestine intelligence activities," as required by the NSL statutory authorities. At present, however, issuing an NSL in the context of a PI will require a waiver or modification of the FCIG. Obtaining such a waiver currently is possible only in international terrorism cases. The FCIG are being revised, but this revision may take some time. Thus, whenever the information sought is relevant to an established full investigation, the field likely will find it more efficient to issue an NSL out of the related full investigation than to request one in a PI.

2. General Policy on the Use of NSL Authority

NSLs are powerful investigative tools, in that they can compel the production of substantial amounts of relevant information. However, they must be used judiciously. The USA PATRIOT Act greatly broadened the FBI's authority to gather this information. However, the provisions of the Act relating to NSLs are subject to a "sunset" provision that calls for the expiration of those provisions in four years. In deciding whether or not to re-authorize the broadened authority, Congress certainly will examine the manner in which the FBI exercised it. Executive Order 12333 and the FCIG require that the FBI accomplish its investigations through the "least intrusive" means. Supervisors should keep this in mind when deciding whether or not a particular use of NSL authority is appropriate. The greater availability of NSLs does not mean that they should be used in every case.

In addition, the removal of any requirement for FBIHQ coordination in the issuing of NSLs creates the possibility of duplicate requests for the same information by different field offices. Field offices must take steps to avoid this. In particular, the field should check FBI databases (ACS, Telephone Application, etc.) and open sources to see if the information sought has already been obtained by the FBI or whether it is publically available. This is particularly important when considering issuing NSLs for telephone or electronic communications data under the Electronic Communications Privacy Act (ECPA). Unlike the criminal authorities in ECPA, the NSL authority does not require the government to reimburse carriers or Internet Service Providers (ISPs) for the cost of producing the requested information. A dramatic increase in duplicate NSLs will only augment existing pressure to require governmental reimbursement.

Individual field offices have the responsibility for establishing and enforcing an appropriate review and approval process for the use of NSL authorities.

3. The Mechanics of Producing NSLs

For all types of NSLs, the issuing office needs to prepare two documents: (1) the NSL itself; and (2) an EC approving the NSL and documenting the predication. Model NSLs and ECs for all variations of the three types of NSLs are included as attachments to this communication. These materials will also be placed on the NSLU Intranet Website and will be distributed by GroupWise e-mail. Once the initial implementation of these new authorities is accomplished, NSLU will work to develop a macro or form to further streamline the NSL process.

A. The NSL

There are presently seven variations of the three NSL types: 1) subscriber information; 2) toll billing records; 3) electronic subscriber information; 4) electronic communication transactional records; 5) financial records; 6) identity of financial institutions; and 7) consumer identifying information. This section will discuss the features that these variations share in common and highlight the differences.

All NSLs must be addressed to an appropriate company point of contact. NSLU will place a list of known points of contact on its intranet website. However, the responsibility for ensuring that the company point of contact is up to date belongs to the drafting field division. Field divisions should advise NSLU of any new points of contact, or when a particular point of contact is no longer valid. Please note that the company point of contact address does not include a zip code, because NSLs must be hand-delivered.

The first paragraph of every NSL provides the appropriate statutory authority for the request, identifies the types of records requested, and provides available identifying information so that the company can process the NSL request. It is this first paragraph that contains the differences that warrant the seven NSL varieties.

Subscriber and electronic subscriber NSLs should have a specific date for each of the phone numbers/e-mail addresses requested. Typically, the specific date is going to be the date that the phone number or e-mail address was used in communication with the subject of the investigation. Any phone numbers identified in a subscriber request should contain all ten digits of the phone number, including the area code.

Toll billing record and electronic communication transactional record requests should have a range of dates for

14

each of the phone numbers/e-mail addresses requested. The date range may be from inception to present, or some other specified date range relevant to the investigation. Any phone numbers identified in a toll billing record request should contain all ten digits of the phone number, including the area code.

Financial record requests should include all available identifying information to facilitate the financial institution's records search. Typically, such identifying information includes: name, account numbers, social security number, and date of birth. The time period for financial record requests is typically from inception of account(s) to present, although a more specific date range may be used.

Credit record requests are similar to financial requests in that they should include available identifying information to facilitate the credit agency's records search. Typically, such identifying information includes: name, social security number, and date of birth. There is no need to specify a date range for credit record requests because these requests seek all records where the consumer maintains or has maintained an account.

The second paragraph of every NSL contains the statutorily required certification language. The certification language is virtually identical for every NSL. However, please note that the certification language used in the financial records NSLs is slightly different than the others in that it states "the records are sought for foreign counterintelligence purposes . . . ." Financial records also contain an additional certification that the FBI has complied with all applicable provisions of the RFPA. Use of the model NSLs will ensure that the proper certifications are made.

The next paragraph contains an admonition for the phone company, ISP, financial institution, or credit agency receiving the NSL. The paragraph warns that no officer, employee, or agent of the company may disclose that the FBI has sought or obtained access to the requested information or records.

The last substantive paragraph instructs the company point of contact to provide the records personally to a representative of the delivering field division. It also states that any questions should be directed to the delivering field division. This last paragraph requires the person preparing the NSL to input the appropriate delivering field division in two places.

The model NSLs for financial records and electronic communication transactional records each have a separate attachment. These attachments provide examples of information which the company might consider to be financial or electronic communication transactional records.

Finally, the NSL is an unclassified document because it does not detail the specific relevance of the requested records to an authorized FBI investigation. There is no need to classify the NSL when attaching it to the cover EC.

B. The Cover EC

The Cover EC serves four essential functions in the NSL process: (1) it documents the predication for the NSL by recording why the information sought is relevant to an investigation; (2) it documents the approval of the NSL by relevant supervisors and the legal review of the document; (3) it contains the information needed to fulfill the Congressional reporting requirements for each type of NSL; and (4) it transmits the NSL to the requesting squad or delivering field division for delivery to the appropriate telecommunications carrier, ISP, financial institution, or credit agency. There are four varieties of model ECs provided with this communication: (1) subscriber/electronic subscriber information; (2) toll billing/electronic communication transactional records; (3) financial records; and (4) credit information. When preparing an NSL request, the field should use one of these model ECs, giving special consideration to the elements discussed in this section.

1) Field Descriptors

This section will generally explain how most of the EC field descriptors should be completed. The "**Precedence**" descriptor will typically be "ROUTINE." The "**Date**" descriptor should reflect the date the NSL and the EC were approved. The "**To**" descriptor will always include "General Counsel" and the requesting squad's field division. It may also include the name of the delivering field division (always Los Angeles in the case of FCRA NSLs) and the office of origin, if applicable. The "**Attn**" descriptor should include the name of the Chief, NSLU, and the squad supervisors and case agents from the requesting squad, delivering field division, and office of origin, if applicable and if known. The credit model EC identifies the FBI personnel working on Squad 4, Santa Ana RA, who are currently responsible for the service of FCRA NSLs. The "**From**" descriptor should identify the certifying official's field division, and include the title of the certifying official. The "**Contact**" descriptor should reflect the name and phone number of the requesting squad case agent. The "**Drafted By**" descriptor should reflect the name of the person who prepared the NSL package. The "**Case ID #**" descriptor must contain the case file number relevant to the request, and the case file numbers indicated in the model EC. The "**Title**" descriptor should list the subject's name, any known aliases, whether the investigation is an FCI or IT investigation directed at a particular foreign power, and identify the office of origin, e.g., *WILLIAM BADGUY, AKA BILL BADGUY, FCI-IRAQ, OO: NEW YORK*. The "**Synopsis**" descriptor should use the standard boilerplate contained in the appropriate model EC. The "**Derived From**" descriptor should be "**G-3**" in bold typeface. The "**Declassify On**" descriptor should be "**X1**" in bold typeface. the "**Full Investigation Instituted**" descriptor should contain the date the full FCI or IT investigation was opened on the subject and indicate whether the subject is a U.S. person. Please note that the word "**Field**" has been deleted from the field descriptor contained in the standard EC macro. In the unlikely event that an NSL is issued during a PI with prior FBIHQ approval, the field descriptor should be edited to state "**Preliminary Inquiry Instituted.**" The remaining descriptors can be filled in according to the model EC being used.

2) Predication and Relevance

The USA PATRIOT Act has greatly simplified the NSL process. The FBI official authorizing the issuance of an NSL is no longer required to certify that there are specific and articulable facts giving reason to believe that the information sought pertains to a foreign power, or an agent of a foreign power. NSLs may now be issued upon a certification of relevance to an authorized investigation to protect against international terrorism or clandestine intelligence activities.

Accordingly, the first paragraph in the "Details" section of the EC should contain the predication for the full investigation and identify the relevance of the requested records to the investigation. Both the predication and relevance should be stated clearly and concisely. The predication should track with the predicates contained in FCIG, Section III.C.1. For example, the predication might state, "A full foreign counterintelligence investigation of subject, a Non-U.S. person, was authorized in accordance with the Attorney General Guidelines because he may be a suspected intelligence officer for the Government of Iraq." Another example might state, "A full international terrorism *investigation of subject, a U.S. person, was authorized in* accordance with the Attorney General Guidelines because he may be engaged in international terrorism activities by raising funds for HAMAS."

The relevance requirement ties the requested records to the appropriate full investigation. For example, relevance could be established by stating, "This subscriber information is being requested to determine the individuals or entities that the subject has been in contact with during the past six months." Another example might state, "The subject's financial records are being requested to determine his involvement in possible HAMAS fund raising activities."

3) Approval

The second paragraph in the "Details" section and the "Approved By" descriptor field of the EC should reflect the level of the official approving the issuance of the EC and signing the NSL's certification. Prior to certification, every NSL and cover EC issued by the field division should be reviewed by the squad supervisor, the Office of the Chief Division Counsel, and the ASAC. Lawyers reviewing NSL packages should use the checklists provided with this communication to ensure legal sufficiency. The last step in the approval process occurs when the certifying official (Deputy Director, ADs, General Counsel, ADICs, DADs, DGC, or SACs) personally signs the NSL and initials the EC. Certifying officials may not further delegate signature authority.

4) Reporting Requirements

NSLU will continue to prepare the mandatory reports to Congress required for each NSL type. To ensure that NSLU receives sufficient information to prepare these reports, it is critical that the person preparing the NSL package follow the NSL and EC models very carefully. The second lead in every model EC requests NSLU to "record the appropriate information needed to fulfill the Congressional reporting requirements for NSLs." NSLU will be able to compile the reporting data provided that the cover EC includes the case file number, the subject's U.S. person status, the type of NSL issued, and the number of phone numbers, e-mail addresses, account numbers, or individual records being requested in the NSL. Once NSLU has entered this reporting data into its NSL database, it will clear the lead set in the cover EC.

5) Transmittal

Often, the squad requesting the NSL will be able to hand-carry the NSL locally to the appropriate company point of contact. However, in many situations, the field division drafting the NSL will have to get it delivered by another field division. In these situations, the drafting division should attempt to identify the squad and personnel at the delivering field division who will be responsible for delivering the NSL. In the event that the office of origin is different than either the drafting division or delivering division, the person drafting the NSL package should ensure that the case agent from the office of origin receives a copy of the package. The first lead in the model ECs should direct the requesting squad or delivering field division to deliver the attached NSL. If the delivering division is different than the drafting division or the office of origin, then this first lead should also request the delivering division to submit the results to the drafting division and/or the office of origin.

4. <u>NSL Preparation Assistance</u>

Some field divisions may, for a variety of reasons, opt not to exercise their delegated authority to issue NSLs. Other field divisions may exceed their capacity to issue NSLs and seek assistance in handling the overflow. NSLU will continue to process any NSL request that it receives. Field divisions should send their requests directly to NSLU, with information copies to the FBIHQ substantive unit. Such requests must contain all the information identified in this communication as necessary to prepare the NSL package. NSLU anticipates that it will be able to process such requests within one to three business days.

Any questions regarding this communication may be directed to [redacted] NSLU, OGC, at [redacted] b7C
[redacted]

b7C-1 b2-1

LEAD(s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Distribute to all supervisory personnel involved in the National Security Letter process.

◆◆

20

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/29/2002

To: Counterterrorism
Counterintelligence

Attn: Section and Unit Chiefs
Section and Unit Chiefs

From: Office of the General Counsel
National Security Law Unit (NSLU)/Room 7975
Contact: [redacted]

Approved By: Bowman M E
Williams Jeff

b7C -1

Drafted By: [redacted]

Case ID #: 66F-HQ-A1247863 (Pending)

Title: PROCEDURAL GUIDANCE RELATED TO
NEW FISA PEN REGISTER AUTHORITY

Synopsis: Summarizes FISA pen register/trap and trace authorities and reiterates procedures for requesting such authority.

Reference: 66F-HQ-A1247863 Serial 70

Administrative: This is a privileged FBI attorney communication; do not circulate outside the FBI without the permission of OGC.

Details: Changes to FISA pen register/trap and trace authorities under the "USA Patriot Act" were summarized in the above referenced electronic communication. In response to requests for clarification of procedures relating to requests for FISA pen register/trap and trace authorities, the National Security Law Unit (NSLU) is providing the following guidance.

<u>I. Legal Basis for Initiation of FISA Pen Register/Trap and Trace</u>

The "USA Patriot Act" revised the legal standard for initiating a FISA pen register/trap and trace.[1] These 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

---

[1] 50 U.S.C. § 1842

11-6-02
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 11-6-02 BY 60267 NLS/EP/CLT
#966750

21

upon the basis of activities protected by the First Amendment to the Constitution."[2]

Use of this technique is authorized in full investigations properly opened under the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG). The FCIG require that full foreign counterintelligence investigations be personally authorized by the relevant Special Agent in Charge, or Assistant Special Agent in Charge with exclusive responsibility for a specific foreign counterintelligence program following written notification to FBIHQ.

II. Process for Obtaining Pen Register/Trap and Trace Authority

No procedural changes were required as the result of revisions made by the "USA Patriot Act." Requests for pen register/trap and trace authority should be submitted with an appropriate letter head memorandum (LHM) to the Counterterrorism Division (CTD) or Counterintelligence Division (CD) unit with management responsibility for the program. The approval of the Unit Chief, Section Chief, and Assistant Director with oversight responsibility is required on the file copy of the LHM. The cognizant unit will forward the LHM to the NSLU, Office of the General Counsel, for legal review. Following approval of the request, the CTD or CD unit will forward the LHM to the Office of Intelligence Policy and Review, U.S. Department of Justice, which will prepare the filing and submit it to the FISA Court. A CTD or CD Supervisory Special Agent will be the affiant verifying the factual content of the application.

The following information should be included in the LHM: the name of subject; field office, case agent, point-of-contact information; type of authority requested (pen register/trap and trace); whether it is an original request or a renewal; a list of the telephone numbers or other communication devices that will be covered by the order along with carrier information; and a brief statement explaining the nature of the investigation and the relevance to that investigation of the information sought through the pen register/trap and trace.

NSLU and OIPR plan to develop additional guidance to further streamline this process. Questions relating to these matters may be directed to Assistant General Counsel [redacted]

LEAD(s):

b7C -1

b2 -1

[2] 50 U.S.C. § 1842(a)(1).

22

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Distribute to relevant personnel involved in FCI/IT investigations.

CC:

◊◊ 1 - Mr. Parkinson
1 - Mr. Bowman
1 - NSLU Attorneys

Documents released by letter dated January 16, 2003

U.S. Department of Justice

Federal Bureau of Investigation
935 Pennsylvania Ave., N.W.
Washington, D.C. 20535-0001

January 16, 2003

Ms. Ann Beeson
American Civil Liberties Union Foundation
125 Broad Street
New York, NY 10004-2400

Subject of Request: ______

FOIPA No. 966750 /190- ______

Dear Requester:

Enclosed are copies of documents from FBI records. Excisions have been made to protect information exempt from disclosure pursuant to Title 5, United States Code, Section 552 (Freedom of Information Act) and/or Section 552a (Privacy Act). In addition, where excisions were made, the appropriate exempting subsections have been cited opposite the deletions. Where pages have been withheld in their entirety, a deleted page information sheet has been substituted showing the reasons or basis for the deletion. The subsections cited for withholding information from the enclosed documents are marked below:

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3) ______	☒ (b)(7)(C)	☐ (k)(1)
______	☐ (b)(7)(D)	☐ (k)(2)
______	☐ (b)(7)(E)	☐ (k)(3)
______	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

(See Form OPCA-16a, enclosed, for an explanation of these exemptions.)

Pursuant to your request, 14 pages(s) were reviewed and 14 page(s) are being released.

During the review of material pertinent to the subject of your request, documents were located which

☐ originated with another Government agency(ies).
These documents were referred to that agency(ies) for review and direct response to you.

☐ contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

☒ If you desire, you may appeal any denials contained herein. Appeals should be directed in writing to the Co-Director, Office of Information and Privacy, U.S. Department of Justice, Flag Building, Suite 570, Washington, D.C. 20530-0001 within sixty days from receipt of this letter. The envelope and the letter should be clearly marked "Freedom of Information Appeal" or "Information Appeal." Please cite the FOIPA number assigned to your request so that it may be easily identified.

☐ The enclosed material is from the main investigative file(s) in which the subject of your request was the subject of the investigation. There are additional references to the subject(s) of your request in files relating to other individuals, organizations, events or activities. These additional mentions or references have not been reviewed to determine if, in fact, they are identifiable with the subject(s) of your request. Our experience has shown that such references are frequently similar to information contained in the processed main file(s). We will process these references if you now make a specific request for them. However, because of a significant increase in FOIPA requests and an expanding backlog, we have given priority to the processing of main investigative files and can only complete the processing of these additional references as time and resources permit.

☒ See additional information which follows.

Sincerely yours,

David M. Hardy/vse

Chief
Freedom of Information-
Privacy Acts Section
Office of Public and Congressional Affairs

Enclosures (3)

This letter supplements our prior responses of November 4, 2002, November 14, 2002 and November 20, 2002.

Enclosed are 12 additional pages which were subsequently located and are responsive to request numbers 2-6 in your letter dated August 21, 2002.

The FBI previously asserted exemption (b)(1) to protect the records sought in request numbers 11 and 12 in that the mere fact of the existence or nonexistence of responsive records is, in and of itself, classified. Upon further review the FBI has determined that we are able to address request numbers 11 and 12. Material which appears to be responsive to request number 12 is maintained in our computer system and we are unable to access it at present. As soon as we are able to gain access to this material it will be processed. We are making every effort to retrieve this information as expeditiously as possible. However, please be advised that we anticipate that the information will be withheld in full pursuant to exemption (b)(1). No information responsive to request number 11 was located.

Top of document.
11/22/02
08:00:29

View Document Text

ECFVTOMO
More : +

Case ID . : 66F-HQ-C1364260 *
Responses :

Serial : 1

Date: 02/08/2002

Precedence: ROUTINE

To: Information Resources Attn: [redacted] Rm. 5334
Investigative Information
Processing Unit

From: Office of the General Counsel
Investigative Law Unit Room 7326
Contact: [redacted] ext. [redacted]

b7c-1
b2-1

Approved By: [redacted]

Command . . . > .... +
F1=Help F3=Exit F4=Prompt F6=Multv F8=Fwd F12=Cancel F13=Attrib F14=List
F15=PrevDoc

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE JAN 7 2003 BY AUC 62033 ckk/H
Comp # 966750

11/2_/02
08:00:37

View Document Text

ECFVTOM0
More : - +

Case ID . : 66F-HQ-C1364260 *
Serial : 1
Responses :

Drafted By: [redacted] b7c-1

Case ID #: 66F-HQ-A1085154

Title: Investigative Law Unit
New File Number
USA Patriot Act

Synopsis: Request opening of a new control file for the Investigative Law Unit's (ILU) Control File to be captioned "USA Patriot Act."

Details: ILU is providing significant guidance to the field on .... +

Command . . . > ....
F1=Help F3=Exit F4=Prompt F6=Multv F7=Bkwd F8=Fwd F12=Cancel F13=Attrib
F14=List F15=PrevDoc

11/22/02 View Document Text ECFVTOM0
08:00:40 More : - +

Case ID . : 66F-HQ-C1364260 * Serial : 1
Responses :

---

various matters related to the recently enacted USA Patriot Act. In order to better capture the work accomplished on this matter, ILU requests that a new control file be opened entitled "USA Patriot Act." All documentation and opinions written by ILU and appropriate documentation collected from others will be filed in this control file.

Any questions regarding this matter should be directed to Assistant General Counsel [redacted] at extension [redacted] b2-1 b7c-1

LEAD (s):

Command . . . > .... +
F1=Help F3=Exit F4=Prompt F6=Multv F7=Bkwd F8=Fwd F12=Cancel F13=Attrib
F14=List F15=PrevDoc

11/22/02 View Document Text ECFVTOMO
08:00:50 More : - +

Case ID . : 66F-HQ-C1364260 * Serial : 1
Responses :

Set Lead 1: (Adm)

INFORMATION RESOURCES

AT WASHINGTON, DC

It is requested that the Investigative Information Processing Unit open a control file captioned "USA Patriot Act."

1 - ILU

Command . . . > .... +
F1=Help F3=Exit F4=Prompt F6=Multv F7=Bkwd F8=Fwd F12=Cancel F13=Attrib
F14=List F15=PrevDoc

11/22/02
07:56:49

View Document Text

ECFVTOM0
More : +

Case ID . : 66F-LR-C41239
Responses :

Serial : 1

Precedence: ROUTINE

Date: 07/29/2002

To: Little Rock

Attn: OSS[redacted]

From: Little Rock

Approved By: [redacted]

b7c-1

Drafted By: [redacted]

Case ID #: 66F-LR-NEW (None)

Command . . . > .... +
F1=Help F3=Exit F4=Prompt F8=Fwd F12=Cancel F13=Attrib F14=List

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE JAN 7 2003 BY AUC 65083 ck/aH
Comp # 966750

11/22/02 View Documei. Text ECFVTOMO
07:58:31 More : - +

Case ID . : 66F-LR-C41239 Serial : 1
Responses :

Title: USA PATRIOT ACT - CONTROL FILE

Synopsis: To request a control file be opened to track the various legislative reporting requirements in the USA PATRIOT ACT.

Details: Because the USA PATRIOT ACT contained many "sunset provisions" (those set to expire on December 31, 2006, without Legislative action), FBIHQ requested all Offices to track the use of certain specific investigative techniques authorized by this statute so that it can report to Congress at the appropriate time. Little Rock employees have been instructed to report the

Command . . . > .... +
F1=Help F3=Exit F4=Prompt F7=Bkwd F8=Fwd F12=Cancel F13=Attrib F14=List

Bottom of document.
11/22/02
07:58:48

View Document Text

ECFVTOMO
More : -

Case ID . : 66F-LR-C41239

Serial : 1

Responses :

---

use of these techniques. At present, the CDC will maintain this control file and do the necessary reporting.

LEAD(s):

Set Lead 1: (Adm)

LITTLE ROCK

AT LITTLE ROCK

Create a control file as set forth above.

Command . . . > .... +
F1=Help F3=Exit F4=Prompt F7=Bkwd F12=Cancel F13=Attrib F14=List

ECFVA1M0 View Document Attributes

Top of document. More : +
ECFVT2M0 View Document Text

Case ID : 40-MD-C530 Serial : 1

Precedence: ROUTINE Date: 06/20/2002

To: Investigative Services Attn: [redacted] OIO/IOU-1

b7c-1
b2-1

From: Madrid
Contact: A/ALAT [redacted]

F1=Help F8=Fwd F12=Cancel F13=Attrib F24=Prt/Dnld

ECFVA1M0 View Document Attributes

ECFVT2M0 View Document Text More : - +

Case ID : 40-MD-C530 Serial : 1

Approved By: [redacted]

b7c-1

Drafted By: [redacted]

Case ID #: 40-MD-C530 (Pending)

Title: VISA APPLICANT NCIC CHECKS

Synopsis: Opening of control file for U.S. Visa and passport matters.

F1=Help F7=Bkwd F8=Fwd F12=Cancel F13=Attrib F24=Prt/Dnld

ECFVA1M0 View Document Attributes

ECFVT2M0 View Document Text More : - +

Case ID : 40-MD-C530 Serial : 1

Reference: PATRIOT ACT and Department of State (DOS) cable, dated 5/24/2002.

Details: With the passage of the Patriot Act, all DOS posts worldwide are required to conduct FBI NCIC traces on all visa applicants. A DOS cable, dated 5/24/2002, stated that beginning June 1, 2002, FBI records were being added to the DOS' CLASS.

The appropriate DOS personnel will now be required to

F1=Help F7=Bkwd F8=Fwd F12=Cancel F13=Attrib F24=Prt/Dnld

ECFVA1M0 View Document Attributes

ECFVT2M0 View Document Text More : - +

Case ID : 40-MD-C530 Serial : 1

fingerprint any individual who is a positive match on any FBI record in the CLASS system. Upon positive confirmation, the DOS personnel will receive criminal history information from the FBI.

If the subject matches a FBI record for a wanted person, foreign fugitive, or member of a violent gang or terrorist organization an immediate EC must be sent to the SIOC and concurrent notification given to the RSO. The Legat and the RSO would then determine the appropriate action.

F1=Help F7=Bkwd F8=Fwd F12=Cancel F13=Attrib F24=Prt/Dnld

ECFVA1M0 View Document Attributes

ECFVT2M0 View Document Text More : - +

Case ID : 40-MD-C530 Serial : 1

LEAD(s):

Set Lead 1:

INVESTIGATIVE SERVICES

AT WASHINGTON, DC

For Information

F1=Help F7=Bkwd F8=Fwd F12=Cancel F13=Attrib F24=Prt/Dnld

report question (providing interim nu s)?

Brown, Jamie E (OLA)

From: O'Brien, Pat
Sent: Thursday, September 05, 2002 6:13 PM
To: Brown, Jamie E (OLA)
Subject: FW:

Translators.wpd

here is the follow up info from FBI on the linguists. we should run this past ODAG (Wray or Laufman) and the AG's office (Taylor and Susan Richmond). Once it is ready, I think we should consider putting it in a letter supplementing our answers.

-----Original Message-----
From: Eleni Kalisch [mailto [redacted]
Sent: Thursday, September 05, 2002 5:55 PM
To: O'Brien, Pat
Subject:

FOIA EXEMPTION per FBI (b)(7)(c)-1

Pat:

Attached are responses to Patriot Act Section 205(c) regarding translators.

Eleni

FOIA EXEMPTION (b)(6) per OIPR

Brown, Jamie E (OLA)

From: Kris, David
Sent: Wednesday, September 04, 2002 1:49 PM
To: Kelly, Patrick (OLA); Colborn, Paul P; Eisenberg, John
Cc: [redacted] O'Brien, Pat; Brown, Jamie E (OLA); Baker, James; Bryant, Dan
Subject: RE: Initial draft of Talkers for Sensenbrenner meeting today (9/4)

My comments:

FOIA EXEMPTION (b)(5) per OIPR

[redacted]

-- David

-----Original Message-----

will be ready -- and whether they can get the information now.

Please let me know if/when we can provide answers to the above. Thanks, Pat

Pat O'Brien
Deputy Assistant Attorney General
Office of Legislative Affairs
U.S. Dept. of Justice
phone (202) 616-6186
fax (202) 514-9149
Pat.O'Brien@usdoj.gov

OUT OF SCOPE

Brown, Jamie E (OLA)

From: Kelly, Patrick
Sent: Wednesday, August 28, 2002 4:40 PM
To: [redacted]
Cc: Brown, Jamie E (OLA)
Subject: HJC letter

FOIA EXEMPTION (b)(6) per OIPR

[redacted]

[redacted] at FBI Congressional Affairs received the letter to HJC and has given it to Spike Bowman for comment. FYI - [redacted] handles Senate and House Judiciary and is Acting Unit Chief in the absence of Eleni and [redacted]. His number - [redacted]

Patrick.

b2-1 FOIA EXEMPTION (b)(7)(c)-1 per FBI

Brown, Jamie E (OLA)

From: Kris, David
Sent: Wednesday, August 28, 2002 1:51 PM
To: [redacted]
Cc: Bryant, Dan; Kelly, Patrick; Brown, Jamie E (OLA)
Subject: RE: Status of draft response to Sesenbrenner subpoena threat

Thanks.

FOIA EXEMPTION (b)(6) per OIPR

-----Original Message-----
From: [redacted]
Sent: Wednesday, August 28, 2002 1:17 PM
To: Kris, David
Cc: Bryant, Dan; Kelly, Patrick; Brown, Jamie E (OLA)
Subject: Status of draft response to Sesenbrenner subpoena threat

FOIA EXEMPTION (b)(5) per OIPR

000842

FYI.

[redacted]

Documents released by letter dated January 31, 2003

U.S. Department o. Justice

Federal Bureau of Investigation
935 Pennsylvania Ave., N.W.

Washington, D.C. 20535-0001

January 31, 2003

Ms. Ann Beeson
American Civil Liberties Union Foundation
125 Board Street
New York, NY 10004-2400

Subject of Request: .

FOIPA No. 966750 /190-

Dear Requester:

Enclosed are copies of documents from FBI records. Excisions have been made to protect information exempt from disclosure pursuant to Title 5, United States Code, Section 552 (Freedom of Information Act) and/or Section 552a (Privacy Act). In addition, where excisions were made, the appropriate exempting subsections have been cited opposite the deletions. Where pages have been withheld in their entirety, a deleted page information sheet has been substituted showing the reasons or basis for the deletion. The subsections cited for withholding information from the enclosed documents are marked below:

Section 552		Section 552a
☒ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☒ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3) ______	☐ (b)(7)(C)	☐ (k)(1)
______	☐ (b)(7)(D)	☐ (k)(2)
______	☒ (b)(7)(E)	☐ (k)(3)
______	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☒ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

(See Form OPCA-16a, enclosed, for an explanation of these exemptions.)

Pursuant to your request, 41 pages(s) were reviewed and 41 page(s) are being released.

During the review of material pertinent to the subject of your request, documents were located which

☐ originated with another Government agency(ies).
These documents were referred to that agency(ies) for review and direct response to you.

☐ contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

☒ If you desire, you may appeal any denials contained herein. Appeals should be directed in writing to the Co-Director, Office of Information and Privacy, U.S. Department of Justice, Flag Building, Suite 570, Washington, D.C. 20530-0001 within sixty days from receipt of this letter. The envelope and the letter should be clearly marked "Freedom of Information Appeal" or "Information Appeal." Please cite the FOIPA number assigned to your request so that it may be easily identified.

☐ The enclosed material is from the main investigative file(s) in which the subject of your request was the subject of the investigation. There are additional references to the subject(s) of your request in files relating to other individuals, organizations, events or activities. These additional mentions or references have not been reviewed to determine if, in fact, they are identifiable with the subject(s) of your request. Our experience has shown that such references are frequently similar to information contained in the processed main file(s). We will process these references if you now make a specific request for them. However, because of a significant increase in FOIPA requests and an expanding backlog, we have given priority to the processing of main investigative files and can only complete the processing of these additional references as time and resources permit.

☐ See additional information which follows.

Sincerely yours,

Chief
Freedom of Information-
Privacy Acts Section
Office of Public and Congressional Affairs

Enclosures (3)

~~SECRET~~

Transactional Records NSLs Since 10/26/2001

Project Number	*NSL to Field Date*
[redacted]	[redacted]

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

b1

(S)

CLASSIFIED DECISIONS FINALIZED
BY DEPARTMENT REVIEW COMMITTEE (DRC)
DATE: 1-29-03 AUC 62033CK/CH
CA# 02-CV-2077

Tuesday, January 21, 2003

Page 1 of 6

Dervied ~~From~~: G-3
Declassify on: X1

~~SECRET~~

JAN 22 2003 AUC 62033
CLASSIFIED BY: CK/CH
REASON: 1.5 (C)
DECLASSIFY ON: X1
CA# 02-CV-2077

38

~~SECRET~~

Project Number	*NSL to Field Date*
[redacted]	[redacted]

b1

(S)

~~Dervied From~~: G-3
~~Declassify on~~: X1

~~SECRET~~

SECRET

Project Number	*NSL to Field Date*
[redacted]	[redacted]

(S)

b1

~~Dervied From: G-3~~
~~Declassify on: X1~~

~~SECRET~~

~~SECRET~~

Project Number	NSL to Field Date
[redacted]	[redacted]

(S) b1

Dervied From: ~~G-3~~
Declassify on: X1
~~SECRET~~

41

SECRET

Project Number	NSL to Field Date
[redacted]	[redacted]

b1

(S)

Dervied From: G-3
Declassify on: X1

SECRET

42

SECRET

Project Number	NSL to Field Date
[redacted]	[redacted] (S)
Grand Total:	[redacted] (S)

b1

Dervied From: G-3
Declassify on: X1
SECRET

SECRET

43

"What do I have to do to get a FISA?"

Introduction

This discussion of the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801 et seq., ("FISA", or "the statute") provides guidance for seeking authorization to conduct electronic surveillance or physical searches for foreign intelligence purposes. In response to the basic question, "What do I have to do to get a FISA?," first, step back and take a look at the big picture. FISA was enacted to provide a statutory procedure for the government to obtain court orders authorizing the use of electronic surveillance in the United States for foreign intelligence purposes. Later, section 807 of the Intelligence Authorization Act for Fiscal Year 1995 (P.L. 103-359) amended FISA to authorize the Court to issue warrants for *physical searches* for foreign intelligence purposes. Accordingly, FISA deals with electronic surveillance and physical searches of foreign powers and their agents. If your purpose is other than the acquisition of foreign intelligence information, as defined by the statute, you're probably in the wrong forum.

Without going into the historical background of FISA in detail, the impetus for its enactment was largely concern for the privacy rights of U.S. persons, balanced against the government's need to obtain foreign intelligence information . As a result, the statute's treatment of "U.S. persons" and "non-U.S. persons" is different. For example, in considering this legislation, Congress stated that a U.S. person should be confident that his government cannot invade his privacy with the most intrusive techniques if he conducts himself lawfully and that, as a matter of public policy, no U.S. person should be targeted for electronic surveillance [or physical search] absent some showing that he at least "may" violate the law. On the other hand, surveillance pursuant to FISA is not primarily for the purpose of gathering evidence of a crime, although evidence of a crime may well be acquired in surveilling persons who engage in the types of activities that define them as agents of foreign powers. As a result, FISA explicitly recognizes that evidence of a crime may be acquired in the course of surveillance or search conducted to protect the United States from the clandestine intelligence activities and international terrorist activities of foreign powers and their agents. Prosecution for a criminal offense is one way to combat such activities -- but only one way, and not always the best way. "Doubling" an agent or feeding him false or useless information are other ways. Monitoring him to discover other agents and their tradecraft can be vitally useful. Prosecution, while disabling one known agent, may only mean that the foreign power replaces him with one whom it may take years to discover or who may never be discovered.

With regard to non-U.S. persons who act in the United States in their official capacities, or who are members of international terrorist groups, however, no nexus to criminality is required, and they are defined as agents of foreign powers solely on the basis of their status. In addition, the retention and dissemination of information concerning non-U.S. persons is signficantly less regulated that that of U.S. person information.

The FISA Court

FISA authorizes the government to apply to a special "Foreign Intelligence Surveillance Court" ("FISC" or "FISA court") for an order approving the use of electronic surveillance or physical search to acquire foreign intelligence information. Pursuant to an October, 2001, amendment by the USA PATRIOT Act, the FISA Court is composed of eleven judges designated by the Chief Justice of the United States. Historically, the judges were chosen from different circuits, but the amendment increasing the number of judges from seven to eleven also specified that they come from seven of the judicial circuits and that no fewer than three shall reside within 20 miles of the District of Columbia.

Approval of a FISA application requires a finding by the court that there is probable cause to believe that the target of the proposed surveillance is a "foreign power" or an "agent of a foreign power," and that the facilities or places at which the surveillance is directed are used or are about to be used by that foreign power or agent of a foreign power. In addition to determining whether there is probable cause to support the application, the Court is also required to find that procedures proposed in the application to regulate the acquisition, retention and dissemination of information concerning U.S. persons meet the definition of "minimization procedures" in section 101(h) of the statute. Because the showing that the target of the proposed surveillance or search is a "foreign power" or an "agent of a foreign power," the definitions of these terms are particularly important. Other terms are also important, including "international terrorism," "foreign intelligence information," "electronic surveillance," "physical search" and "United States person," all of which are defined in section 101 or 301 of the statute and will be discussed in detail, *infra*.

Subsection 105(a) of FISA specifies the findings the court must make before he grants an order approving the use of electronic surveillance for foreign intelligence purposes. While the issuance of an order is mandatory if the court finds that all of the requirements of this section are met, the judge has the discretionary power to modify the order sought, such as with regard to the period of authorization or the minimization procedures to be followed. In practice, the FISA Court has found general supervisory powers in this language, and its power to modify minimization procedures has been used as power to influence or control other aspects of investigations. This is essentially what the Court did in its April 22 and May 17 orders in construing discussions between intelligence officials and law enforcement officials about investigative strategies and tactics as "minimization procedures" that required OIPR attendance to ensure that such discussions did not result in and in requiring OIPR be invited to attend.

Probable Cause . . .

In general terms, FISA deals with "foreign powers" and "agents of foreign powers," and the fundamental requirement for the Court's granting a FISA application is probable cause to believe that the proposed subject of surveillance or search is a foreign power or an agent thereof. "Foreign power" includes a foreign government; a faction of a foreign government; a group engaged in international terrorism; a foreign-based political organization; or an entity directed and controlled by a foreign government or governments. An "agent of a foreign power" includes non-resident aliens who act in the United States as officers, members or employees of foreign powers, or who act on behalf of foreign powers that engage in clandestine intelligence activities in the United States contrary to the interests of this country. U.S. persons meet the "agent of a foreign power" criteria if they engage in certain activities for or on behalf of a foreign power which involve, or may involve, certain criminal acts.

Subsection 105(a)(3) provides that in order to issue an order for electronic surveillance, the Court must find that on the basis of the facts submitted by the applicant there is "probable cause" to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power and that each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Subsection 304(a)(3) provides for similar findings with regard to physical search. As to both electronic surveillance and physical searches, no United States person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the First Amendment to the Constitution.

Probable cause in the FISA context is similar to, but not the same as, probable cause in criminal cases. Where a U.S. person is believed to be an agent of a foreign power, there must be probable cause to believe that he is engaged in certain activities, for or on behalf of a foreign power, which activities involve or may involve a violation of U.S. criminal law. The phrase "involve or may involve" indicates that the showing of [nexus to] criminality does not apply to FISA applications in the same way it does to ordinary criminal cases. As a result, there is no showing or finding that a crime has been or is being committed, as in the case of a search or seizure for law enforcement purposes. The activity identified by the government in the FISA context may not yet involve criminality, but if a reasonable person would believe that such activity is likely to lead to illegal activities, that would suffice. In addition, and with respect to the nexus to criminality required by the definitions of "agent of a foreign power," the government need not show probable cause as to each and every element of the crime involved or about to be involved.

The determination as to probable cause to believe that a target is engaging in certain activities, or that an entity is directed and controlled by a foreign government, should take into account the same aspects of reliability of the government's information as in the ordinary criminal context, including the reliability of any informant, the circumstances of the informant's knowledge and the age of the information relied upon. On the other hand, not all of the same strictures with respect to these matters which have developed in the criminal context may be appropriate in the foreign intelligence context. That is, in the criminal context certain rules have developed or may develop for judging reliability of information. FISA does not require that these "rules" necessarily be applied to the probable cause determination. Rather, in judging the reliability of the information presented by the government, look to the totality of the information and consider its reliability on a case-by-case basis.

In *Illinois v. Gates*, 462 U.S. 213 (1983), the Supreme Court overruled rigid application of the two-pronged test for the reliability of an informant set forth in *Spinelli v United States*, 393 U.S. 410 (1969). *Spinelli* required both knowledge of the source of an informant's information as well as information as to the reliability of a source before his information could used to establish probable cause. *Gates* acknowledged that it was appropriate to consider such factors as instructive, but they should not be applied with mathematical precision. As a result, *Gates* stands for a "totality-of-the-circumstances" approach.

Also instructive is the case of *Brinegar v. United States*, 338 U.S. 160 (1949), which noted that probable cause is a factual and practical consideration of everyday life on which reasonable and prudent men act, not legal technicians. At the same time, probable cause is based on a presentation of reliable and corroborated facts, not mere suspicion.

Simply put, "probable cause" is reason to believe, based on available facts and circumstances, as well as the logical inferences that can be drawn from them. It is determined by the totality of the facts and circumstances, as viewed from the perspective of a reasonable person. Probable cause probability, not certainty, and, thus, is significantly lower than the "proof beyond a reasonable doubt" necessary to support a criminal conviction. It is also lower than the "preponderance of the evidence" required in most civil cases.

NSLU recommends that a field agent seeking a FISA order focus on the *object* of the belief required, *i.e.*, the facts and circumstances demonstrating that the target of the proposed search or surveillance is an agent of a foreign power and that the premises to be surveilled (*e.g.*, telephone) is used by that agent of a foreign power, rather than on the *quantum* of the belief involved. If you can show that a target is engaged in certain activities, and that he is engaged in them for or on behalf of a foreign power, you have won most of the battle.

No U.S. person may be considered an agent of a foreign power based solely on activities protected by the First Amendment to the Constitution. This provision is intended to reinforce the congressional intent that lawful political activities should never be the sole basis for a finding that a U.S. person is a foreign power or an agent thereof. For example, under the Supreme Court's decision in *Brandenburg v. Ohio*, 395 U.S. 444 (1969), the advocacy of violence, falling short of inciting violence, is protected by the First Amendment. Thus, advocating the commission of terrorist acts would not, in and of itself, be sufficient to establish probable cause to believe that an individual or group may be preparing to commit such acts. However, one cannot cloak himself in First Amendment immunity where he is engaged in clandestine intelligence activities, terrorism or sabotage. ["The Constitution is not a suicide pact."]

. . . Probable Cause to Believe What?

To find probable cause to believe the subject of the surveillance is an "agent of a foreign power," as defined in subsection 101(b), the court must find that each and every element of that status exists. If a U.S. person is alleged to be acting on behalf of a foreign entity, the court must first find probable cause to believe that that entity is a "foreign power," as defined in subsection 101(a). There must also be probable cause to believe that the person is acting "for or on behalf of" that foreign power, as well as probable cause to believe that the efforts undertaken by the target on behalf of the foreign power constitute sabotage, international terrorism or clandestine intelligence activities. Similar findings are required for each element necessary to establish that a U.S. person is conspiring with or aiding and abetting someone engaged in sabotage, international terrorism or clandestine intelligence activities.

The Theory of the Case

The development of a "theory of the case" is a good start to the FISA process. That is, before asking FBIHQ for initiation of an application to the FISA Court, the field agent should review the facts of the case to determine which definition of "foreign power" and/or "agent of a foreign power" best matches the information obtained by the investigation to date. For example, if the subject is a U.S. person who is believed to be knowingly engaged in aiding and abetting an international terrorist, focus on facts that show his activities that aid the terrorist, as well as on facts that tend to demonstrate his knowledge that the person he is aiding is an international terrorist and that his activities aid that international terrorist. If the subject is a non-U.S. person who acts in the U.S. as an employee of a foreign government, focus on presenting facts that demonstrate that status. In such a case, a recitation of intelligence activities is not as important as it would be in the case of a U.S. person, as to whom the FBI would have to show facts demonstrating knowing engagement in clandestine intelligence activities.

It is also helpful to articulate the specific foreign intelligence objectives of the proposed surveillance or search. In an espionage case, *e.g.*, your objective may be to determine whom an intelligence officer has targeted for recruitment. Or you may need to know how a government employee is communicating with an intelligence officer who is his handler. Or you may need to determine the identity of a foreign power a spy is working for, how he obtains access to classified information, whether he is working alone or in concert with others and how he passes information to his handler. In an international terrorism case, your objectives may include identifying the members of the terrorist group or identifying their plans and intentions in order to prevent a terrorist attack.

§ 101(b) -- Agent of a foreign power

Probably the single most important aspect of the request for a FISA application is showing that the subject to be surveilled or searched is an "agent of a foreign power." The definitions of "agent of a foreign power" differ for U.S. persons and certain non-resident aliens, including aliens present in the United States as tourists, visiting businessmen, exchange visitors, foreign seamen, diplomatic and consular personnel and illegal aliens, etc. The protections afforded such persons are not as great as those afforded U.S. persons. For example, in the case of non-resident aliens who a.e agents of foreign powers by virtue of their employment in the U.S. by a foreign government, there need be no nexus to criminality, and the certification that accompanies the application is not subject to judicial review. In addition, there is no requirement to minimize the acquisition, retention and dissemination of information with respect to non-U.S. persons.

§ 101(b)(1) -- Non-U.S. Persons Who Are Agents of a Foreign Power by Virtue of Status

Subsection 101(b)(1)(A) includes in its definition of "agent of a foreign power" non-U.S. persons who act in the United States as officers, employees or members of a foreign power. The most obvious examples are diplomats and consular officials. Their very presence is attributable to their status as employees of their governments, and their *raison d'etre* is to act for or on behalf their governments. The legislative history of FISA points out that Congress considers non-resident aliens who act in the United States as officers, employees or members of a foreign power as likely sources of foreign intelligence or counterintelligence information. This definition does not include persons who serve as officers or employees or are members of a foreign power in their home country, but who do not act in that capacity in the United States.

"Employee" is meant to describe a normal employee-employer relationship. It does not encompass foreign visitors such as professors, lecturers, exchange students, performers or athletes, even if in such capacity they are receiving remuneration or expenses from their home government.

The term "member" means an active, knowing member of a group or organization that is a foreign power. It does not include mere sympathizers, fellow-travelers or persons who have merely attended meetings of the group or organization. On the other hand, if a person has received terrorist training from a group engaged in international terrorism or training in intelligence tradecraft from a foreign organization, this would be substantial evidence that he was a "member" of such an entity.

Unlike foreign officials, members of international terrorist groups do not carry membership cards as evidence of their status. They do not have visas or credentials identifying them as "members" of an IT group or organization. As a result, their status as members of a group or organization engaged in international terrorism is inferred from their activities.

The second non-U.S. person definition is the so-called "visitor rule." It includes a non-U.S. person who --

> acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engaged in such activities.

This definition does not require a showing that the foreign visitor is in fact engaged in clandestine intelligence activities. As a practical matter, if a foreign visitor who does not have a track record of activities in the United States is present in the U.S. for only a limited period of time, and the FBI is limited to the use of less intrusive techniques, the FBI is not likely to be able to show that he is actually engaged in intelligence or terrorist activities. He can be characterized as an agent of a foreign power, however, if it can be shown that the foreign power on whose behalf he acts systematically engages in clandestine intelligence [or terrorist] activities that threaten the security of the United States. It is a demonstration based on *probability; i.e.*, it is not a showing that the individual foreign visitor is himself currently engaged in clandestine intelligence activities, but that the *circumstances* of his presence in the U.S. indicate he *may* engage in such activities because the foreign power for whom or on whose behalf he acts has demonstrated some pattern or practice of engaging in clandestine intelligence activities in the United States contrary to U.S. interests.

The phrase "acts for or on behalf of a foreign power" requires a nexus between the individual and the foreign power that suggests that he is likely to do the bidding of the foreign power. For example, visitors from totalitarian countries present in the United States under the auspices, sponsorship or direction of their government would satisfy this standard.

Once the requisite facts with regard to the foreign power are established, the key question is whether the circumstances of the person's presence in the U.S. indicate that he may engage in clandestine intelligence activities for that foreign power contrary to U.S. interests. The answer may vary according to what is known about the intelligence or terrorist operations of the particular foreign power. Among the factors that might be taken into account are whether the foreign visitor engages in activities with respect to which there is evidence that other visitors who engage in similar activities are officers, agents or acting on behalf of the intelligence service of that foreign power. If the FBI can show from experience that a particular foreign power uses a certain class of visitors to this country for carrying out secret intelligence assignments, this would indicate that other visitors in this class may also engage in clandestine intelligence activities.

"May engage in such activities" means that surveillance can be conducted to *anticipate* clandestine intelligence activities by such persons, rather than waiting until they have taken place. The additional standards for aiding and abetting, and conspiracy, require probable cause to believe that the foreign visitor is knowingly assisting persons who are already engaged in clandestine intelligence activities. The "knowing" requirements are the same as in the aiding or abetting and conspiracy standard for U.S. persons.

This provision does *not* treat nationals of certain countries differently from others solely on the basis of nationality, and it is *not* "profiling." Instead, surveillance of the nationals of certain countries depends on the *activities* of the governments of those countries and whether the individual is *acting on behalf of* the government.

"Any Person" Agent of a Foreign Power

§ 101(b)(2)(A) -- Clandestine Intelligence Gathering Activities

Under this definition, an agent of a foreign power is "any person who is knowingly engaged in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal laws of the United States."

The first aspect of this definition is that the subject is engaging in certain activities "knowingly." This does not mean that he must know that he may be violating a particular federal criminal statute, but that he knows that what he is doing is clandestine intelligence gathering activities and that he knows that he is doing it for or on behalf of a foreign power. As state of mind is always difficult to show, knowledge is inferred from the circumstances. In showing that a person is knowingly engaged in clandestine intelligence gathering activities, focus on his *activities*. If, for example, a subject is transmitting classified defense secrets to the military attache of a foreign embassy, and he knows the information is classified and that his recipient is a military attache, this would be sufficient to show that he "knows" that he is acting for or on behalf of a foreign power. Similarly, if he has received training in the use of equipment for espionage, *e.g.*, a microdot camera or disguised radio device, this would be sufficient to show that he "knows" what he is doing. One who is unwitting to what he is doing, or without knowledge that he is acting for or on behalf of a foreign power, is not an agent of a foreign power, but the government is not required to pro... ignorance if a person engaging in such activities would reasonably have known that he was acting for or on behalf of a foreign power.

Next, the person must be "engaged" in the proscribed activities. Unlike the standard for foreign visitors, the fact that he "may engage" in such activities some time in the future is not sufficient. For example, if information shows that a person has recently engaged in such activities, this would normally suffice to show probable cause that he is "engaged." On the other hand, information that a person engaged in the prohibited activities in the past might well, depending on the circumstances, be sufficient to show probable cause to believe that he is still engaged in such activities. For example, information that a U.S. person was for years a spy for a foreign power hostile to the United States, but who had dropped out of sight for a few years, would probably be sufficient to show "probable cause" that he was, having now reappeared, continuing to engage in the clandestine intelligence activities.

Perhaps the most important element of this definition is "clandestine intelligence gathering activities." Most clandestine intelligence gathering activities will constitute a violation of the various federal criminal laws aimed at espionage either directly or by failure to register (see, *e.g.*, 18 U.S.C. §§ 792-799, 951; 42 U.S.C. §§ 2272-2278b; and 50 U.S.C. § 855). The term "clandestine intelligence gathering activities" is intended to mean "espionage" in common parlance; it is not a legal term of art denoting a particular offense. The term also includes activities that are directly supportive of espionage, such as maintaining a "safehouse," servicing "letter drops," running an "accommodation address," laundering funds, recruiting new agents, infiltrating or exfiltrating agents under cover, creating false documents for an agent's "cover" or utilizing a radio to receive or transmit instructions or information by "burst transmission." The term "clandestine intelligence gathering activities" is intended to mean activities in which no reasonable person would engage without knowing that society would not condone it.

As the words indicate, the activities must be "clandestine," *i.e.*, the subject must have made some efforts to conceal his activities. This does not necessarily mean that the information gathered by the agent must itself be secret or nonpublic, although this is usually the case. It is possible that a person might be asked to obtain information that is publicly available, but which a foreign power would not want known it was seeking. If he used false identification or ruse to obtain the information and then delivered the information by means of a microdot hidden in a magazine left at a "dead drop," both the means by which he gathered the information and the means by which he transmitted it would be "clandestine," even though the information itself might not be secret. The FBI may surveil such a person, even if the information he is collecting is not classified, because his activities identify him as an agent of a foreign power. By monitoring his contacts, their equipment and *modus operandi*, the FBI can learn valuable information concerning the tactics, capabilities and personnel of the foreign intelligence service.

"Clandestine intelligence gathering activities" are intended to be conduct of a nature associated with spies and espionage in its generic sense, but the term is supposed to be flexible with respect to what is being gathered because intelligence priorities and requirements differ between nations and over time. Obviously, gathering classified defense information, information about intelligence sources and methods and classified foreign relations information qualifies as "clandestine intelligence gathering activities" if it is done in a clandestine manner. Foreign powers also target American technology and trade secrets, economic developments, political information and even personal information for purposes of blackmail or other coercion, so that attempts to collect such information may also be "clandestine intelligence gathering activities."

It is possible, although unlikely, that some people might come close to using espionage techniques for otherwise lawful purposes. Thus, the definition requires that the person be engaged in clandestine intelligence gathering activities "for or on behalf of a foreign power." The fact that a person gathers information and transmits it to a foreign power does not, by itself, satisfy the requirements of this definition, as people may legitimately gather information for foreign powers. Registered lobbyists, *e.g.*, often do, but their activity, if legitimate, does not utilize the tradecraft of espionage or clandestine methods, to do so. This means that the FBI must show probable cause to believe that the person is not only engaged in clandestine intelligence gathering activities, but that he is doing so for or on behalf of a foreign power. Thus, showing that a person is stealing defense secrets and using a "dead drop" to pass them on is not enough; it must be shown that he is doing so for a foreign power.

The FBI must show that there is probable cause to believe that a subject is engaged in activity that at least "may" violate a federal criminal statute. As noted above, it is expected that most persons under this definition would be likely to violate laws directed against espionage. There are other laws, however, that might be violated, such as interstate transportation of stolen property or the Export Administration Act. The crime involved might be one of several violations depending, for example, upon the nature of the information being gathered.

The words "may involve" are intended to encompass clandestine intelligence gathering activities that may, as an integral part of such activities, involve a violation of federal law. They cover the situation in which the FBI cannot establish probable cause to believe that a foreign agent's activities involve a specific criminal act, but where there are specific and articulable facts to indicate that a crime may be involved. The circumstances might be such as to indicate that the activity may involve a crime. The term "may involve" requires only limited information regarding the crime involved, such that electronic surveillance may be permissible at some point prior to the time a crime, *e.g.*, the passage of classified documents, actually occurs. There need not be a current or imminent violation of law if there is probable cause to believe that criminal acts may be committed.

In applying this standard, the FISA Court takes all the known relevant circumstances into account, *e.g.*, who the subject is, where he is employed, whether he has access to classified or other sensitive information, the nature of clandestine meetings or other clandestine activity, the method of transmission and whether there are innocent explanations for the behavior. The circumstances must not merely be suspicious, but must be of such a nature to lead a reasonable man to conclude that the activity may involve a federal criminal violation.

Again, a nexus to a foreign power is absolutely necessary. Surveillance would not be authorized against a reporter merely because he gathers information for publication in a newspaper, even if the information were classified. Nor would it be authorized against a government employee who reveals secrets to a reporter or in a book for the purpose of informing the public. This definition would not authorize surveillance of ethnic Americans who lawfully gather political information and perhaps even lawfully share it with the foreign government of their national origin. Nor would it apply to lawful activities to lobby, influence or inform members of Congress or the Administration to take certain positions with respect to foreign or domestic concerns. Nor would it apply to lawful gathering of information prepatory to such lawful activities. It is the combination of (1) obtaining in clandestine fashion (2) information that is necessary to the defense or security of the United States (3) for or on behalf of a foreign power that makes FISA surveillance

In the case of an organization whose leaders are engaged in clandestine intelligence gathering activities, such activity cannot necessarily be attributed to every member of the group. There must be probable cause to believe that a particular member is himself engaged in such activity before electronic surveillance targeted against him may be authorized.

Because the standard under this definition requires that a person knowingly engage in activities for or on behalf of a foreign power, problems can arise in a situation in which a person is "turned" or "doubled," *i.e.*, after having started out as an agent for a foreign power, he is persuaded to work for the United States. The standard is not met if the person is in fact working for the U.S. and not for the foreign power. There may be doubt, however, as to whether he is actually under U.S. control or that of a foreign power, making it unclear as to which side is deceiving which. The fact that a supposedly "doubled" agent carries out his assignments and instructions from the U.S. Government does not necessarily mean that he has stopped carrying out those of the foreign power. It is not necessary, therefore, that a surveillance, once authorized, be discontinued when the agent may have been "doubled." Rather, surveillance may continue until such time as the "doubled" agent is trusted enough to seek his consent to surveillance.

§ 101(b)(2)(B) -- "Other Clandestine Intelligence Activities"

Subsection 101(b)(2)(B) defines agent of a foreign power as a person who pursuant to the direction of an intelligence service or network of a foreign power knowingly engages in "other clandestine intelligence activities" for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States. ["Other" refers to other than clandestine intelligence *gathering* activities.]

The term refers to covert actions by intelligence services of foreign powers. Not only do foreign powers engage in spying in the United States to obtain information, they also engage in activities that are intended to harm U.S. security by affecting the course of government, the course of public opinion or the activities of individuals. Such activities may include political action (recruiting, bribery or influencing public officials to act in favor of the foreign power), disguised propaganda (including the planting of false or misleading articles or stories) and harassment, intimidation or even assassination of individuals who oppose the foreign power. Such activity can undermine democratic institutions as well as directly threaten the peace and safety of U.S. citizens.

There may be a narrow line between clandestine intelligence activities and lawful activities undertaken by U.S. persons in the exercise of First Amendment rights. To avoid crossing that line, this definition requires that the person be shown to be acting "pursuant to the direction of an intelligence service or network of a foreign power." [No such showing is required for the other definitions of agent of a foreign power.] U.S. persons may well communicate with a foreign government to obtain information about that government's country or to discuss travel to that country, but such contacts are not necessarily "clandestine intelligence activities" and are not covered by this definition.

The activities engaged in must involve, or be about to involve, a violation of federal criminal law. This is higher than the "may" involve standard found in other definitions. In this area, where there is a narrow line between protected First Amendment activity and the activity giving rise to surveillance, it is important that the activity be such that it involves or is about to involve a violation of a federal criminal statute.

There are a number of crimes that might be involved in covert action, *e.g.*, bribery of public officials, campaign law violations, foreign agent registration requirements, denial of civil rights, *et cetera*. It is important to note, however, that such a criminal violation does not necessarily establish that a person is engaged in "other clandestine intelligence activity." Americans, through ignorance or inadvertence, may well technically violate campaign law requirements or foreign agent registration requirements, but to satisfy the requirements of the definition, it is necessary to show, separately from the criminal violation, probable cause to believe that the person is knowingly engaged in any other clandestine intelligence activities for or on behalf of such foreign power, *pursuant to the direction of an intelligence service or network of a foreign power.*

§ 101(b)(2)(C) -- Sabotage or Terrorism

Subsection 101(b)(2)(C) allows electronic surveillance or physical search of any person, including a U.S. person, who knowingly engages in sabotage or international terrorism, or activities in preparation therefor, for or on behalf of a foreign power. The terms "sabotage" and "international terrorism" are defined separately and require a showing of criminal activity. Mere sympathy for, identity of interest with or vocal support for the goals of a foreign group, even a foreign-based terrorist group, is not sufficient to justify surveillance under this subparagraph. The term "activities that are in preparation [for]" sabotage or international terrorism is intended to encompass activities supportive of acts of serious violence -- for example, purchase or surreptitious importation into the United States of explosives, planning for assassinations or financing of or training for such activities. Other activities supportive of terrorist acts could likewise satisfy this standard. The circumstances must be such as would lead a reasonable person to conclude that the subject is knowingly engaged in activities that are in preparation for sabotage or terrorism.

The term "preparation" does not mean preparation for a specific terrorist act. Because the definition of "international terrorism" speaks of a range of acts, and "preparation" as used here takes its meaning from the context of the definition of "international terrorism," it could reasonably be interpreted to include, *e.g.*, providing the personnel, training, funding or other means for the commission of acts of terrorism, rather than participating in a particular bombing. This provision also permits electronic surveillance or physical search at a time *before* the danger sought to be prevented -- whether a kidnaping, bombing or hijacking -- actually occurs.

The "preparation" standard allows surveillance where the government cannot establish that an individual has already knowingly engaged in an act of sabotage or terrorism, but there are sufficient specific and articulable facts to indicate that his activities are in preparation for such acts. The circumstances must be such as would lead a reasonable person to conclude that the subject is knowingly engaged in activities that are in preparation for sabotage or terrorism.

It should be noted that the "preparation" standard need apply only where there is insufficient information to show that the subject is, in fact, a terrorist. Where the FBI can show that the subject is a known international terrorist, such as the notorious "Carlos," or that he has been engaging in international terrorism for or on behalf of a group engaged in international terrorism, there is no need to show that he is in the act of preparing for further terrorist acts. In some cases, immediate arrest may not be possible, such as situations in which the subject may not have violated U.S. law, even though he may have murdered hundreds of persons abroad. In other cases it may be more fruitful to monitor the subject's activities in the United States to identify otherwise unknown terrorists located here, their international support structure and the locations of weapons or explosives. If a person who has engaged in international terrorism visits the U.S. or resides in the U.S., the FBI should be able to utilize electronic surveillance to monitor his activities, whether or not there is information showing that he is presently planning some particular violent act.

Finally, a subject targeted for surveillance under this definition must be shown to have a knowing connection with the foreign power for whom he is working. In most cases of international terrorism, this connection will be shown to exist with a group engaged in international terrorism. The case may arise in which a U.S. person is acting for or on behalf of such a group that is substantially composed of U.S. persons. In such a case, the Court must examine the circumstances carefully in order to determine whether the organization is "a group engaged in international terrorism," as defined, and not a purely domestic group engaged in domestic terrorism. [Domestic terrorism is handled under criminal law processes, *e.g.*, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Title 18, U.S. Code, chapter 119, and the AG Guidelines for General Crimes.]

§101(b)(2)(D) -- Entering the U.S. under a False or Fraudulent Identity

This definition includes any person who knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power. The most obvious example would be the "illegal" who enters the United States under an assumed name and using a "legend" based on the vital statistics of a real person, usually dead. It would also include a person who enters the United States lawfully, then assumes a false identity, provided assuming such a false identity is done for or on behalf of a foreign power.

§101(b)(2)(E) -- Aiding, Abetting and Conspiracy

This definition includes any person, including a U.S. person, who knowingly aids or abets any person in the conduct of activities described in the preceding subsections, or knowingly conspires with any person to engage in such activities. The knowledge requirement is applicable to both the status of the person being aided and the nature of the activity being promoted. This means the FBI must establish probable cause to believe that the subject knows both that the person with whom he is conspiring or whom he is aiding or abetting is engaged in the described activities as an agent of a foreign power and that his own conduct is assisting or furthering such activities. The innocent dupe who unwittingly aids a foreign intelligence officer cannot be targeted under this provision.

In the case of a subject believed to be aiding or abetting persons engaged in international terrorism, the subject might be assisting a group engaged in both lawful political activity and unlawful terrorist acts. In such a case, it would be necessary to establish probable cause to believe that he was aware of the terrorist activities undertaken by the group and was knowingly furthering them, not merely that he was aware of and furthering the group's lawful activity.

Verification Procedures

[redacted]

b2-2
b5-1
b7E-1

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] b2-2 b5-1 b7E-1

[redacted]

[redacted]

FISA Court's Rule 11

By order dated May 17, 2002, the FISA Court promulgated "Rule 11, Criminal Investigations in FISA Cases":

> All FISA applications shall include informative descriptions of any ongoing criminal investigations of FISA targets, as well as the substance of any consultations between the FBI and criminal prosecutors at the Department of Justice or a United States Attorney's Office.

Rule 11 formalizes the requirement for descriptions of any ongoing criminal investigation, an issue that was addressed in the "verification procedures" dated April 5, 2001. Then Rule 11 adds the requirement to describe the substance of any consultations between the FBI and criminal prosecutors at DOJ or a United States Attorney's Office. The scope and degree of such consultations have proliferated significantly since promulgation of the AG's memo on information sharing on March 6, 2002, and access by prosecutors to intelligence information and to case files on intelligence investigations has reached unprecedented proportions [redacted]

[redacted]

b2-2
b5-1
b7E-1

[redacted]

[redacted]

b2-2
b5-1
b7E-1

Certification

Subsection 104(a)(7) of FISA requires a certification by the Assistant to the President for National Security Affairs -- or other Executive Branch official designated by the President from among those officials employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate. The designated presidential advisor is the only one specifically provided for in the statute. By Executive Orders 12139 and 12949 the President has also designated the Director (and Deputy) of Central Intelligence, the Secretary (and Deputy) of Defense, the Secretary (and Deputy) of State and the Director of the FBI. Note that the Deputy Director of the FBI is conspicuously absent -- the Deputy Director is typically a career Special Agent rather than an official appointed by the President with the advice and consent of the Senate and therefore does not meet the statutory prerequisites.

Foreign Intelligence Information

The certification consists of five elements, the first of which is that the official making the certification deems the information sought to be foreign intelligence information. If you relate these officials and their functions to the definition of "foreign intelligence information" in section 101(e) of the statute, there is a certain attraction of logic in their selection. Under subsection 101(e)(1), "foreign intelligence information" means information that relates to [or, if concerning a United States person, is *necessary* to] the ability of the United States to protect against (a) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (b) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (c) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power. These elements go to the classic counterintelligence and counterterrorism functions of the CIA and the FBI.

Under subsection 101(e)(2), the definition of "foreign intelligence information" includes information with respect to a foreign power or foreign territory that relates to [or, if concerning a United States person, is *necessary* to] (a) the national defense or the security or (B) the conduct of the foreign affairs of the United States. These elements implicate the missions and functions of the Secretary of Defense and the Secretary of State.

Under the scheme set up by Executive Order 12333, the Assistant to the President for National Security Affairs (the "National Security Advisor") is the senior Executive Branch official in the Intelligence Community and has interests in *all* of these matters.

The requirement that the certifier deems the information sought to be "foreign intelligence information" is designed to ensure that a senior official with responsibilities in the area of national security reviews the determination made at lower levels of the Executive Branch that the information sought is foreign intelligence information. The intent of FISA is ensure that the certifier carefully considers the substance of cases before him and does not simply sign off on boilerplate language. This prevents targeting a foreign power for electronic surveillance when the true purpose is to gather information about an individual for other than foreign intelligence purposes. It is also designed to make explicit that a significant purpose of such surveillance is to obtain "foreign intelligence information" as defined, rather than some other type of information. The certifier similarly must explain in his affidavit why the information cannot be obtained through less intrusive techniques. This requirement is particularly important when U.S. persons are the targets of surveillance or search.

A Significant Purpose

The second element of the certification is that "a significant purpose" of the surveillance or search is to obtain foreign intelligence information. Since the objective in enacting the statute is to provide a statutory procedure for the government to obtain a judicial order for electronic surveillance or physical search for foreign intelligence purposes, the "purpose" aspect of the certification is extremely important. The majority of pre-FISA caselaw had recognized a "national security exception" to the warrant requirement of the Fourth Amendment. In determining whether the cases before them should be accorded that exception, the courts tended to focus on whether the collection of foreign intelligence information was the "primary" purpose of the surveillance. In the case of Humphrey and Truong the trial judge concluded that the fruits of electronic surveillance and physical searches conducted without a warrant were admissible under the Fourth Amendment, provided those surveillances and searches had been conducted for a foreign intelligence purpose. The measure by which he determined purpose was direction and control of the surveillance, or investigation. So long as special agents of the FBI who normally investigated intelligence activities were directing and controlling the investigation, he construed the information as having been obtained for a foreign intelligence purpose. Conversely, when DOJ prosecutors began to write prosecutive memoranda and to control the direction of the investigation, he concluded that the information had been obtained for the purpose of prosecution and, accordingly, was inadmissible since it had been obtained without a warrant.

When FISA was enacted, it required that "the purpose" of the surveillance be to obtain foreign intelligence information. Based on experience with pre-FISA caselaw, the government's practice before the Foreign Intelligence Surveillance Court has been to construe "the purpose" as "primary purpose" and to determine purpose by following a procedure similar to that adopted in

Humphrey and Truong. A reading of the legislative history of FISA suggests that subsection 104(a)(7) was intended to replace the *Humphrey-Truong* test with the accountable official's certification that the purpose of the surveillance or search is to acquire foreign intelligence information, as defined. The USA PATRIOT Act amended FISA to require that obtaining foreign intelligence information be a "significant" purpose of the surveillance or search. While there is a dearth of legislative history of this amendment, it would appear that the Congress intended to rectify perceived lapses in the government's handling of certain counterintelligence investigations with regard to the determination of probable cause to believe that he was an agent of a foreign power and to steer the government -- as well as the Foreign Intelligence Surveillance Court -- toward the statutory scheme of relying on the certification for determining purpose.

The information required by the FISC's Rule 11 is largely a recitation of criminal justice pursuits and appears to follow the pre-enactment practice of determining purpose through an examination of direction and control of the investigation. The Court's position in this regard was reiterated in its opinions of April 22 and May 17, 2002, regarding the AG's March 6, 2002, memo on information sharing. The certification required by subsection 104(a)(7) is not so much an analysis of direction and control as an affirmation of the intelligence objectives of the surveillance or search. The point for field agents to understand is that in submitting a request for initiation of FISA surveillance or search, it is important to articulate the specific intelligence objectives of the requested FISA coverage. *E.g.*, in an espionage case, those objectives might include identification of a subject's handler, or his tradecraft in servicing dead-drops or how he obtains access to classified information. In the case of a terrorism subject, the objectives of the surveillance might be to learn the extent of the subject's relationship with an international terrorist group. To ensure that the Director has a proper basis for making this certification, NSLU recommends that any communication to HQ requesting application to the Court for authorization to use a FISA technique should both articulate the intelligence objectives to be achieved through the use of FISA techniques and, to satisfy requirements imposed by the Court, describe any criminal aspect of the investigation in sufficient detail to determine that intelligence officials and not law enforcement officials are directing and controlling the use of FISA techniques.

Not Reasonably Obtainable by Other Means

The third element of the certification is that the information sought cannot reasonably be obtained by normal investigative techniques. There is not much legislative guidance on this requirement, but, in general terms, it appears to is based on the general principle -- subsequently reiterated in Executive Order 12333 -- that the Intelligence Community should respect individual privacy rights by conducting intelligence activities using the least intrusive techniques feasible. Thus, it would appear that, due to their intrusiveness, Congress intended FISA techniques should be a last -- rather than first -- resort. In most instances, this requirement can be satisfied by the fact that only surveillance or search of the kind authorized pursuant to FISA can adequately obtain the information sought. For example, if more visible or detectable means of surveillance were utilized, the subject would likely change his means of communication to something less susceptible of surveillance.

Category of Foreign Intelligence Information Sought

The fourth aspect of the certification is designation of the type of foreign intelligence information being sought according to the categories described in section 101(e) of the statute, whether one of the kinds of counterintelligence information defined in subsection 101(e)(1), or of positive intelligence as defined in subsection 101(e)(2).

Basis for Certification

The final part of the certification is a statement of the basis for the certification as to the third and fourth elements, *i.e.*, that the information sought is the type of foreign intelligence information designated, and that such information cannot reasonably be obtained by normal investigative techniques. Usually this is based on the results of the FBI's investigation to date. A presentation of facts relevant to this issue might follow a logical flow of relating the activities of the target that make him an "agent of a foreign power" as defined in subsection 101(b) to the appropriate definition of "foreign intelligence information" in subsection 101(e), coupled with a discussion of the technique that would be necessary to obtain that kind of intelligence information. This element of the certification is not required when the target of the electronic surveillance is a foreign power as defined in subsection 801(a)(1), (2) or (3), *i.e.*, a foreign government or component thereof; a faction of a foreign nation not substantially composed of United States persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.

Duration

The general rule is that the FISC may approve electronic surveillance for the period necessary to achieve its purpose, or for 90 days, whichever is less. There are certain exceptions. Electronic surveillance of a foreign power as defined in section 101(a)(1), (2) or (3) may be authorized for up to one year. Electronic surveillance of a foreign agent as defined in section 101(b)(1)(A) may be for the period specified in the application or for 120 days, whichever is less. Upon renewal, surveillance of a 101(b)(1)(A) agent of a foreign power may be for a period not to exceed one year.

An order authorizing physical search may be approved for the period necessary to achieve its purpose, or for 90 days, whichever is less. As with electronic surveillance, there are exceptions. Physical search of a foreign power, as defined in 101(a)(1), (2) or (3), may be authorized for the period specified in the application or for one year, whichever is less, and physical search of a section 101(b)(1)(A) agent of a foreign power may be authorized for the period specified in the application or for 120 days, whichever is less. An extension may be granted for a period not to exceed one year if the judge finds probable cause to believe that no property of any individual United States person will be acquired during the period in which search is authorized.

It is important to ensure that surveillance or searches adhere to the timelines specified in the orders. For one thing, the length of time involved in drafting a FISA application and preparing it for presentation to the Court requires that requests for renewal be forwarded in timely fashion. You cannot wait until two weeks before an order expires to submit a request for the next one. It is also imperative that actual surveillance or search not occur beyond the period of authorization specified in the order. If surveillance should overrun the period of authorization, any unauthorized "take" must be sequestered and forwarded to the Office of Intelligence Policy and Review, via the substantive unit at FBIHQ, for submission to the Foreign Intelligence Surveillance Court. The overrun must also be reported by electronic communication to the Inspection Management Unit of the Inspection Division within 14 days of discovery of the error. [See section 2-56.E of the National Foreign Intelligence Program Manual.]

Miscellaneous Considerations

Getting an order from the Court is only the beginning of the successful administration of the authorities granted pursuant to FISA. Among the practical considerations that should attend implementation of a FISA order is ensuring that the "premises" being surveilled are those named in the order. For example, it is important to ensure that telephone coverage is on the right telephone line. Clues that something is amiss might include the fact that intercepted communications are in a language other than that expected. Or the information obtained might appear to be non-pertinent to the intelligence objectives of the surveillance.

In cases of physical search, the Court typically requires a return by the federal officer executing the search. The return is essentially a report to the Court of the circumstances under which the search was conducted and the information or tangible items seized. It is common for the Court to require a return within twenty-one (21) days of the execution of a search, but 21 days is not necessarily applicable to all cases, so it is important to note the specific requirements of individual orders.

Another practical consideration is the provision of subsection 105(c)(2) that the Court may order a communications common carrier, landlord, custodian or other specified person to furnish the applicant [the FBI] with all information, facilities or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy. In addition, the Court may order such persons maintain any records concerning the surveillance or the aid furnished that such person wishes to retain under security procedures approved by the Attorney General and the Director of Central Intelligence. Subsection 304(c)(2) makes similar provision for physical searches.

A recurring problem is service of the order on service providers or other specified persons who lack security clearances or, in some cases, the wherewithal to store classified orders properly. When FISA was originally enacted, the overwhelming bulk of the surveillance was simple telephone wiretaps, and there were only a few large communications common carriers with which to deal. As a result, it was relatively easy to obtain clearances for a security office at a large carrier to obtain proper access to information and storage facilities. Since then, however, the large telephone companies have broken up into numerous "baby bells," leading to a proliferation of the workload involved with background investigations and clearances. In addition, the advent of the Internet and the concomitant proliferation of Internet service providers have also added to investigative and security clearance workloads.

The security procedures approved by the Attorney General and the Director of Central Intelligence empower the SAC to authorize disclosure of a classified order on an emergency basis under circumstances in which such disclosure is necessary to execute the order. As a rule, the classified information contained in a secondary order is typically limited to identification of the target -- which information is frequently communicated to the service provider anyway in preliminary discussion. As a result, showing a service provider the secondary order typically amounts to disclosure of something he already knows -- the identity of the subject of surveillance. In a case in which an ongoing relationship is not likely and there is no need for the service provider to have longterm access to classified information, the SAC may authorize showing the secondary order to a service provider or other specified person on a one-time basis. It is recommended that the service provider be offered a "trust receipt" that relates back to the order by date and docket number and that the field office secure the secondary order. The service provider should be advised that the order will be made available should the need arise. If needed, a copy of the security procedures [which are classified] and a model trust receipt may be obtained from NSLU via Groupwise e-mail.

With regard to the trust receipt, the most common concern expressed by service providers is the fear of being sued for providing assistance to the FBI. Service providers may be advised of the following provision of subsection 105(i):

> No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any

information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act for electronic surveillance or physical search.

In addition to this statutory protection from civil liability, if a service provider were to be sued for assisting the FBI in conducting electronic surveillance or physical search pursuant to FISA, the Bureau would seek the Attorney General's assertion of the State Secrets Privilege [United States v. Reynolds, 345 U.S. 1 (1953)] to prevent the disclosure of classified information that would be required to sustain such a cause of action. If a field office is contacted by a service provider about such a situation, NSLU should be notified immediately.

Coming Attractions . . .

The gathering of information, including information as to the capabilities, intentions and activities of foreign powers and their agents, would be meaningless without successful exploitation of that information to protect the United States from hostile attack and other grave acts, acts of terrorism, sabotage and clandestine intelligence activities. Bearing in mind that the recurring theme in various provisions of FISA is the balancing of individual rights to privacy against the need of the government's need to acquire and produce foreign intelligence information, FISA creates a heavy burden with regard to managing the acquisition, retention and dissemination of U.S. person information. In sum, this is the process of "minimization." As most minimization procedures are classified, minimization is not addressed here in detail. In addition, the procedures for "information sharing" promulgated by the Attorney General on March 6 and modified somewhat by the FISA Court are still subject to judicial review. Accordingly, procedures for the sharing of information will be the subject of a separate communication.

Top of Page

Last Updated:

FISA/Info Sharing > FISA Recipe

"What do I have to do to get a FISA?"

Introduction

This discussion of the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801 et seq., ("FISA", or "the statute") provides guidance for seeking authorization to conduct electronic surveillance or physical searches for foreign intelligence purposes. In response to the basic question, "What do I have to do to get a FISA?," first, step back and take a look at the big picture. FISA was enacted to provide a statutory procedure for the government to obtain court orders authorizing the use of electronic surveillance in the United States for foreign intelligence purposes. Later, section 807 of the Intelligence Authorization Act for Fiscal Year 1995 (P.L. 103-359) amended FISA to authorize the Court to issue warrants for *physical searches* for foreign intelligence purposes. Accordingly, FISA deals with electronic surveillance and physical searches of foreign powers and their agents. If your purpose is other than the acquisition of foreign intelligence information, as defined by the statute, you're probably in the wrong forum.

Without going into the historical background of FISA in detail, the impetus for its enactment was largely concern for the privacy rights of U.S. persons, balanced against the government's need to obtain foreign intelligence information . As a result, the statute's treatment of "U.S. persons" and "non-U.S. persons" is different. For example, in considering this legislation, Congress stated that a U.S. person should be confident that his government cannot invade his privacy with the most intrusive techniques if he conducts himself lawfully and that, as a matter of public policy, no U.S. person should be targeted for electronic surveillance [or physical search] absent some showing that he at least "may" violate the law. On the other hand, surveillance pursuant to FISA is not primarily for the purpose of gathering evidence of a crime, although evidence of a crime may well be acquired in surveilling persons who engage in the types of activities that define them as agents of foreign powers. As a result, FISA explicitly recognizes that evidence of a crime may be acquired in the course of surveillance or search conducted to protect the United States from the clandestine intelligence activities and international terrorist activities of foreign powers and their agents. Prosecution for a criminal offense is one way to combat such activities -- but only one way, and not always the best way. "Doubling" an agent or feeding him false or useless information are other ways. Monitoring him to discover other agents and their tradecraft can be vitally useful. Prosecution, while disabling one known agent, may only mean that the foreign power replaces him with one whom it may take years to discover or who may never be discovered.

With regard to non-U.S. persons who act in the United States in their official capacities, or who are members of international terrorist groups, however, no nexus to criminality is required, and they are defined as agents of foreign powers solely on the basis of their status. In addition, the retention and dissemination of information concerning non-U.S. persons is signficantly less regulated that that of U.S. person information.

The FISA Court

FISA authorizes the government to apply to a special "Foreign Intelligence Surveillance Court" ("FISC" or "FISA court") for an order approving the use of electronic surveillance or physical search to acquire foreign intelligence information. Pursuant to an October, 2001, amendment by the USA PATRIOT Act, the FISA Court is composed of eleven judges designated by the Chief Justice of the United States. Historically, the judges were chosen from different circuits, but the amendment increasing the number of judges from seven to eleven also specified that they come from seven of the judicial circuits and that no fewer than three shall reside within 20 miles of the District of Columbia.

Approval of a FISA application requires a finding by the court that there is probable cause to believe that the target of the proposed surveillance is a "foreign power" or a[illegible]gent of a foreign power," and that the facilities or places at which the surveillance is directed are used or are about to be used by that foreign power or agent of a foreign power. In addition to determining whether there is probable cause to support the application, the Court is also required to find that procedures proposed in the application to regulate the acquisition, retention and dissemination of information concerning U.S. persons meet the definition of "minimization procedures " in section 101(h) of the statute. Because the showing that the target of the proposed surveillance or search is a "foreign power" or an "agent of a foreign power," the definitions of these terms are particularly important. Other terms are also important, including "international terrorism," "foreign intelligence information," "electronic surveillance," "physical search" and "United States person," all of which are defined in section 101 or 301 of the statute and will be discussed in detail, *infra*.

Subsection 105(a) of FISA specifies the findings the court must make before he grants an order approving the use of electronic surveillance for foreign intelligence purposes. While the issuance of an order is mandatory if the court finds that all of the requirements of this section are met, the judge has the discretionary power to modify the order sought, such as with regard to the period of authorization or the minimization procedures to be followed. In practice, the FISA Court has found general supervisory powers in this language, and its power to modify minimization procedures has been used as power to influence or control other aspects of investigations. This is essentially what the Court did in its April 22 and May 17 orders in construing discussions between intelligence officials and law enforcement officials about investigative strategies and tactics as "minimization procedures" that required OIPR attendance to ensure that such discussions did not result in and in requiring OIPR be invited to attend.

Probable Cause . . .

In general terms, FISA deals with "foreign powers" and "agents of foreign powers," and the fundamental requirement for the Court's granting a FISA application is probable cause to believe that the proposed subject of surveillance or search is a foreign power or an agent thereof. "Foreign power" includes a foreign government; a faction of a foreign government; a group engaged in international terrorism; a foreign-based political organization; or an entity directed and controlled by a foreign government or governments. An "agent of a foreign power" includes non-resident aliens who act in the United States as officers, members or employees of foreign powers, or who act on behalf of foreign powers that engage in clandestine intelligence activities in the United States contrary to the interests of this country. U.S. persons meet the "agent of a foreign power" criteria if they engage in certain activities for or on behalf of a foreign power which involve, or may involve, certain criminal acts.

Subsection 105(a)(3) provides that in order to issue an order for electronic surveillance, the Court must find that on the basis of the facts submitted by the applicant there is "probable cause" to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power and that each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Subsection 304(a)(3) provides for similar findings with regard to physical search. As to both electronic surveillance and physical searches, no United States person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the First Amendment to the Constitution.

Probable cause in the FISA context is similar to, but not the same as, probable cause in criminal cases. Where a U.S. person is believed to be an agent of a foreign power, there must be probable cause to believe that he is engaged in certain activities, for or on behalf of a foreign power, which activities involve or may involve a violation of U.S. criminal law. The phrase "involve or may involve" indicates that the showing of [nexus to] criminality does not apply to FISA applications in the same way it does to ordinary criminal cases. As a result, there is no showing or finding that a crime has been or is being committed, as in the case of a search or seizure for law enforcement purposes. The activity identified by the government in the FISA context may not yet involve criminality, but if a reasonable person would believe that such activity is likely to lead to illegal activities, that would suffice. In addition, and with respect to the nexus to criminality required by the definitions of "agent of a foreign power," the government need not show probable cause as to each and every element of the crime involved or about to be involved.

The determination as to probable cause to believe that a target is engaging in certain activities, or that an entity is directed and controlled by a foreign government, should take into account the same aspects of reliability of the government's information as in the ordinary criminal context, including the reliability of any informant, the circumstances of the informant's knowledge and the age of the information relied upon. On the other hand, not all of the same strictures with respect to these matters which have developed in the criminal context may be

64

appropriate in the foreign intelligence context. That is, in the criminal context certain rules have developed or may develop for judging reliability of information. FISA does not require that the "rules" necessarily be applied to the probable cause determination. Rather, in judging the reliability of the information presented by the government, look to the totality of the information and consider its reliability on a case-by-case basis.

In *Illinois v. Gates*, 462 U.S. 213 (1983), the Supreme Court overruled rigid application of the two-pronged test for the reliability of an informant set forth in *Spinelli v United States*, 393 U.S. 410 (1969). *Spinelli* required both knowledge of the source of an informant's information as well as information as to the reliability of a source before his information could used to establish probable cause. *Gates* acknowledged that it was appropriate to consider such factors as instructive, but they should not be applied with mathematical precision. As a result, *Gates* stands for a "totality-of-the-circumstances" approach.

Also instructive is the case of *Brinegar v. United States*, 338 U.S. 160 (1949), which noted that probable cause is a factual and practical consideration of everyday life on which reasonable and prudent men act, not legal technicians. At the same time, probable cause is based on a presentation of reliable and corroborated facts, not mere suspicion.

Simply put, "probable cause" is reason to believe, based on available facts and circumstances, as well as the logical inferences that can be drawn from them. It is determined by the totality of the facts and circumstances, as viewed from the perspective of a reasonable person. Probable cause probability, not certainty, and, thus, is significantly lower than the "proof beyond a reasonable doubt" necessary to support a criminal conviction. It is also lower than the "preponderance of the evidence" required in most civil cases.

NSLU recommends that a field agent seeking a FISA order focus on the *object* of the belief required, *i.e.*, the facts and circumstances demonstrating that the target of the proposed search or surveillance is an agent of a foreign power and that the premises to be surveilled (*e.g.*, telephone) is used by that agent of a foreign power, rather than on the *quantum* of the belief involved. If you can show that a target is engaged in certain activities, and that he is engaged in them for or on behalf of a foreign power, you have won most of the battle.

No U.S. person may be considered an agent of a foreign power based solely on activities protected by the First Amendment to the Constitution. This provision is intended to reinforce the congressional intent that lawful political activities should never be the sole basis for a finding that a U.S. person is a foreign power or an agent thereof. For example, under the Supreme Court's decision in *Brandenburg v. Ohio*, 395 U.S. 444 (1969), the advocacy of violence, falling short of inciting violence, is protected by the First Amendment. Thus, advocating the commission of terrorist acts would not, in and of itself, be sufficient to establish probable cause to believe that an individual or group may be preparing to commit such acts. However, one cannot cloak himself in First Amendment immunity where he is engaged in clandestine intelligence activities, terrorism or sabotage. ["The Constitution is not a suicide pact."]

. . . Probable Cause to Believe What?

To find probable cause to believe the subject of the surveillance is an "agent of a foreign power," as defined in subsection 101(b), the court must find that each and every element of that status exists. If a U.S. person is alleged to be acting on behalf of a foreign entity, the court must first find probable cause to believe that that entity is a "foreign power," as defined in subsection 101(a). There must also be probable cause to believe that the person is acting "for or on behalf of" that foreign power, as well as probable cause to believe that the efforts undertaken by the target on behalf of the foreign power constitute sabotage, international terrorism or clandestine intelligence activities. Similar findings are required for each element necessary to establish that a U.S. person is conspiring with or aiding and abetting someone engaged in sabotage, international terrorism or clandestine intelligence activities.

The Theory of the Case

The development of a "theory of the case" is a good start to the FISA process. That is, before asking FBIHQ for initiation of an application to the FISA Court, the field agent should review the facts of the case to determine which definition of "foreign power" and/or "agent of a foreign power" best matches the information obtained by the investigation to date. For example, if the subject is a U.S. person who is believed to be knowingly

65

the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engaged in such activities.

This definition does not require a showing that the foreign visitor is in fact engaged in clandestine intelligence activities. As a practical matter, if a foreign visitor who does not have a track record of activities in the United States is present in the U.S. for only a limited period of time, and the FBI is limited to the use of less intrusive techniques, the FBI is not likely to be able to show that he is actually engaged in intelligence or terrorist activities. He can be characterized as an agent of a foreign power, however, if it can be shown that the foreign power on whose behalf he acts systematically engages in clandestine intelligence [or terrorist] activities that threaten the security of the United States. It is a demonstration based on *probability; i.e.*, it is not a showing that the individual foreign visitor is himself currently engaged in clandestine intelligence activities, but that the *circumstances* of his presence in the U.S. indicate he *may* engage in such activities because the foreign power for whom or on whose behalf he acts has demonstrated some pattern or practice of engaging in clandestine intelligence activities in the United States contrary to U.S. interests.

The phrase "acts for or on behalf of a foreign power" requires a nexus between the individual and the foreign power that suggests that he is likely to do the bidding of the foreign power. For example, visitors from totalitarian countries present in the United States under the auspices, sponsorship or direction of their government would satisfy this standard.

Once the requisite facts with regard to the foreign power are established, the key question is whether the circumstances of the person's presence in the U.S. indicate that he may engage in clandestine intelligence activities for that foreign power contrary to U.S. interests. The answer may vary according to what is known about the intelligence or terrorist operations of the particular foreign power. Among the factors that might be taken into account are whether the foreign visitor engages in activities with respect to which there is evidence that other visitors who engage in similar activities are officers, agents or acting on behalf of the intelligence service of that foreign power. If the FBI can show from experience that a particular foreign power uses a certain class of visitors to this country for carrying out secret intelligence assignments, this would indicate that other visitors in this class may also engage in clandestine intelligence activities.

"May engage in such activities" means that surveillance can be conducted to *anticipate* clandestine intelligence activities by such persons, rather than waiting until they have taken place. The additional standards for aiding and abetting, and conspiracy, require probable cause to believe that the foreign visitor is knowingly assisting persons who are already engaged in clandestine intelligence activities. The "knowing" requirements are the same as in the aiding or abetting and conspiracy standard for U.S. persons.

This provision does *not* treat nationals of certain countries differently from others solely on the basis of nationality, and it is *not* "profiling." Instead, surveillance of the nationals of certain countries depends on the *activities* of the governments of those countries and whether the individual is *acting on behalf of* the government.

"Any Person" Agent of a Foreign Power

§ 101(b)(2)(A) -- Clandestine Intelligence Gathering Activities

Under this definition, an agent of a foreign power is "any person who is knowingly engaged in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal laws of the United States."

The first aspect of this definition is that the subject is engaging in certain activities "knowingly." This does not mean that he must know that he may be violating a particular federal criminal statute, but that he knows that what he is doing is clandestine intelligence gathering activities and that he knows that he is doing it for or on behalf of a foreign power. As state of mind is always difficult to show, knowledge is inferred from the circumstances. In showing that a person is knowingly engaged in clandestine intelligence gathering activities, focus on his *activities*. If, for example, a subject is transmitting classified defense secrets to the military attache of a foreign embassy, and he knows the information is classified and that his recipient is a military attache, this would be sufficient to show that he "knows" that he is acting for or on behalf of a foreign power. Similarly, if he has received training in the use of equipment for espionage, *e.g.*, a microdot camera or disguised radio device, this would be sufficient to show that he "knows" what he is doing. One who is unwitting to what he is doing, or

67

engaged in aiding and abetting an international terrorist, focus on facts that show his activities that aid the terrorist, as well as on facts that tend to demonstrate his knowledge that the person he is aiding is an international terrorist and that his activities aid that international terrorist. If the subject is a non-U.S. person who acts in the U.S. as an employee of a foreign government, focus on presenting facts that demonstrate that status. In such a case, a recitation of intelligence activities is not as important as it would be in the case of a U.S. person, as to whom the FBI would have to show facts demonstrating knowing engagement in clandestine intelligence activities.

It is also helpful to articulate the specific foreign intelligence objectives of the proposed surveillance or search. In an espionage case, *e.g.*, your objective may be to determine whom an intelligence officer has targeted for recruitment. Or you may need to know how a government employee is communicating with an intelligence officer who is his handler. Or you may need to determine the identity of a foreign power a spy is working for, how he obtains access to classified information, whether he is working alone or in concert with others and how he passes information to his handler. In an international terrorism case, your objectives may include identifying the members of the terrorist group or identifying their plans and intentions in order to prevent a terrorist attack.

§ 101(b) -- Agent of a foreign power

Probably the single most important aspect of the request for a FISA application is showing that the subject to be surveilled or searched is an "agent of a foreign power." The definitions of "agent of a foreign power" differ for U.S. persons and certain non-resident aliens, including aliens present in the United States as tourists, visiting businessmen, exchange visitors, foreign seamen, diplomatic and consular personnel and illegal aliens, etc. The protections afforded such persons are not as great as those afforded U.S. persons. For example, in the case of non-resident aliens who are agents of foreign powers by virtue of their employment in the U.S. by a foreign government, there need be no nexus to criminality, and the certification that accompanies the application is not subject to judicial review. In addition, there is no requirement to minimize the acquisition, retention and dissemination of information with respect to non-U.S. persons.

§ 101(b)(1) -- Non-U.S. Persons Who Are Agents of a Foreign Power by Virtue of Status

Subsection 101(b)(1)(A) includes in its definition of "agent of a foreign power" non-U.S. persons who act in the United States as officers, employees or members of a foreign power. The most obvious examples are diplomats and consular officials. Their very presence is attributable to their status as employees of their governments, and their *raison d'etre* is to act for or on behalf their governments. The legislative history of FISA points out that Congress considers non-resident aliens who act in the United States as officers, employees or members of a foreign power as likely sources of foreign intelligence or counterintelligence information. This definition does not include persons who serve as officers or employees or are members of a foreign power in their home country, but who do not act in that capacity in the United States.

"Employee" is meant to describe a normal employee-employer relationship. It does not encompass foreign visitors such as professors, lecturers, exchange students, performers or athletes, even if in such capacity they are receiving remuneration or expenses from their home government.

The term "member" means an active, knowing member of a group or organization that is a foreign power. It does not include mere sympathizers, fellow-travelers or persons who have merely attended meetings of the group or organization. On the other hand, if a person has received terrorist training from a group engaged in international terrorism or training in intelligence tradecraft from a foreign organization, this would be substantial evidence that he was a "member" of such an entity.

Unlike foreign officials, members of international terrorist groups do not carry membership cards as evidence of their status. They do not have visas or credentials identifying them as "members" of an IT group or organization. As a result, their status as members of a group or organization engaged in international terrorism is inferred from their activities.

The second non-U.S. person definition is the so-called "visitor rule." It includes a non-U.S. person who --

> acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in

66

without knowledge that he is acting for or on behalf of a foreign power, is not an agent of a foreign power, but the government is not required to prove ignorance if a person engaging in such activities would reasonably have known that he was acting for or on behalf of a foreign power.

Next, the person must be "engaged" in the proscribed activities. Unlike the standard for foreign visitors, the fact that he "may engage" in such activities some time in the future is not sufficient. For example, if information shows that a person has recently engaged in such activities, this would normally suffice to show probable cause that he is "engaged." On the other hand, information that a person engaged in the prohibited activities in the past might well, depending on the circumstances, be sufficient to show probable cause to believe that he is still engaged in such activities. For example, information that a U.S. person was for years a spy for a foreign power hostile to the United States, but who had dropped out of sight for a few years, would probably be sufficient to show "probable cause" that he was, having now reappeared, continuing to engage in the clandestine intelligence activities.

Perhaps the most important element of this definition is "clandestine intelligence gathering activities." Most clandestine intelligence gathering activities will constitute a violation of the various federal criminal laws aimed at espionage either directly or by failure to register (see, *e.g.*, 18 U.S.C. §§ 792-799, 951; 42 U.S.C. §§ 2272-2278b; and 50 U.S.C. § 855). The term "clandestine intelligence gathering activities" is intended to mean "espionage" in common parlance; it is not a legal term of art denoting a particular offense. The term also includes activities that are directly supportive of espionage, such as maintaining a "safehouse," servicing "letter drops," running an "accommodation address," laundering funds, recruiting new agents, infiltrating or exfiltrating agents under cover, creating false documents for an agent's "cover" or utilizing a radio to receive or transmit instructions or information by "burst transmission." The term "clandestine intelligence gathering activities" is intended to mean activities in which no reasonable person would engage without knowing that society would not condone it.

As the words indicate, the activities must be "clandestine," *i.e.*, the subject must have made some efforts to conceal his activities. This does not necessarily mean that the information gathered by the agent must itself be secret or nonpublic, although this is usually the case. It is possible that a person might be asked to obtain information that is publicly available, but which a foreign power would not want known it was seeking. If he used false identification or ruse to obtain the information and then delivered the information by means of a microdot hidden in a magazine left at a "dead drop," both the means by which he gathered the information and the means by which he transmitted it would be "clandestine," even though the information itself might not be secret. The FBI may surveil such a person, even if the information he is collecting is not classified, because his activities identify him as an agent of a foreign power. By monitoring his contacts, their equipment and *modus operandi*, the FBI can learn valuable information concerning the tactics, capabilities and personnel of the foreign intelligence service.

"Clandestine intelligence gathering activities" are intended to be conduct of a nature associated with spies and espionage in its generic sense, but the term is supposed to be flexible with respect to what is being gathered because intelligence priorities and requirements differ between nations and over time. Obviously, gathering classified defense information, information about intelligence sources and methods and classified foreign relations information qualifies as "clandestine intelligence gathering activities" if it is done in a clandestine manner. Foreign powers also target American technology and trade secrets, economic developments, political information and even personal information for purposes of blackmail or other coercion, so that attempts to collect such information may also be "clandestine intelligence gathering activities."

It is possible, although unlikely, that some people might come close to using espionage techniques for otherwise lawful purposes. Thus, the definition requires that the person be engaged in clandestine intelligence gathering activities "for or on behalf of a foreign power." The fact that a person gathers information and transmits it to a foreign power does not, by itself, satisfy the requirements of this definition, as people may legitimately gather information for foreign powers. Registered lobbyists, *e.g.*, often do, but their activity, if legitimate, does not utilize the tradecraft of espionage or clandestine methods, to do so. This means that the FBI must show probable cause to believe that the person is not only engaged in clandestine intelligence gathering activities, but that he is doing so for or on behalf of a foreign power. Thus, showing that a person is stealing defense secrets and using a "dead drop" to pass them on is not enough; it must be shown that he is doing so for a foreign power.

The FBI must show that there is probable cause to believe that a subject is engaged in activity that at least "may" violate a federal criminal statute. As noted above, it is expected that most persons under this definition would be likely to violate laws directed against espionage. There are other laws, however, that might be violated,

68

such as interstate transportation of stolen property or the Export Administration Act. The crime involved might be one of several violations depending, for example, upon the nature of the information being gathered.

The words "may involve" are intended to encompass clandestine intelligence gathering activities that may, as an integral part of such activities, involve a violation of federal law. They cover the situation in which the FBI cannot establish probable cause to believe that a foreign agent's activities involve a specific criminal act, but where there are specific and articulable facts to indicate that a crime may be involved. The circumstances might be such as to indicate that the activity may involve a crime. The term "may involve" requires only limited information regarding the crime involved, such that electronic surveillance may be permissible at some point prior to the time a crime, *e.g.*, the passage of classified documents, actually occurs. There need not be a current or imminent violation of law if there is probable cause to believe that criminal acts may be committed.

In applying this standard, the FISA Court takes all the known relevant circumstances into account, *e.g.*, who the subject is, where he is employed, whether he has access to classified or other sensitive information, the nature of clandestine meetings or other clandestine activity, the method of transmission and whether there are innocent explanations for the behavior. The circumstances must not merely be suspicious, but must be of such a nature to lead a reasonable man to conclude that the activity may involve a federal criminal violation.

Again, a nexus to a foreign power is absolutely necessary. Surveillance would not be authorized against a reporter merely because he gathers information for publication in a newspaper, even if the information were classified. Nor would it be authorized against a government employee who reveals secrets to a reporter or in a book for the purpose of informing the public. This definition would not authorize surveillance of ethnic Americans who lawfully gather political information and perhaps even lawfully share it with the foreign government of their national origin. Nor would it apply to lawful activities to lobby, influence or inform members of Congress or the Administration to take certain positions with respect to foreign or domestic concerns. Nor would it apply to lawful gathering of information prepatory to such lawful activities. It is the combination of (1) obtaining in clandestine fashion (2) information that is necessary to the defense or security of the United States (3) for or on behalf of a foreign power that makes FISA surveillance

In the case of an organization whose leaders are engaged in clandestine intelligence gathering activities, such activity cannot necessarily be attributed to every member of the group. There must be probable cause to believe that a particular member is himself engaged in such activity before electronic surveillance targeted against him may be authorized.

Because the standard under this definition requires that a person knowingly engage in activities for or on behalf of a foreign power, problems can arise in a situation in which a person is "turned" or "doubled," *i.e.*, after having started out as an agent for a foreign power, he is persuaded to work for the United States. The standard is not met if the person is in fact working for the U.S. and not for the foreign power. There may be doubt, however, as to whether he is actually under U.S. control or that of a foreign power, making it unclear as to which side is deceiving which. The fact that a supposedly "doubled" agent carries out his assignments and instructions from the U.S. Government does not necessarily mean that he has stopped carrying out those of the foreign power. It is not necessary, therefore, that a surveillance, once authorized, be discontinued when the agent may have been "doubled." Rather, surveillance may continue until such time as the "doubled" agent is trusted enough to seek his consent to surveillance.

§ 101(b)(2)(B) -- "Other Clandestine Intelligence Activities"

Subsection 101(b)(2)(B) defines agent of a foreign power as a person who pursuant to the direction of an intelligence service or network of a foreign power knowingly engages in "other clandestine intelligence activities" for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States. ["Other" refers to other than clandestine intelligence *gathering* activities.]

The term refers to covert actions by intelligence services of foreign powers. Not only do foreign powers engage in spying in the United States to obtain information, they also engage in activities that are intended to harm U.S. security by affecting the course of government, the course of public opinion or the activities of individuals. Such activities may include political action (recruiting, bribery or influencing public officials to act in favor of the foreign power), disguised propaganda (including the planting of false or misleading articles or stories) and harassment, intimidation or even assassination of individuals who oppose the foreign power. Such activity can undermine democratic institutions as well as directly threaten the peace and safety of U.S. citizens.

There may be a narrow line between clandestine intelligence activities and lawful activities undertaken by U.S. persons in the exercise of First Amendment rights. To avoid crossing that line, this definition requires that the person be shown to be acting "pursuant to the direction of an intelligence service or network of a foreign power." [No such showing is required for the other definitions of agent of a foreign power.] U.S. persons may well communicate with a foreign government to obtain information about that government's country or to discuss travel to that country, but such contacts are not necessarily "clandestine intelligence activities" and are not covered by this definition.

The activities engaged in must involve, or be about to involve, a violation of federal criminal law. This is higher than the "may" involve standard found in other definitions. In this area, where there is a narrow line between protected First Amendment activity and the activity giving rise to surveillance, it is important that the activity be such that it involves or is about to involve a violation of a federal criminal statute.

There are a number of crimes that might be involved in covert action, *e.g.*, bribery of public officials, campaign law violations, foreign agent registration requirements, denial of civil rights, *et cetera*. It is important to note, however, that such a criminal violation does not necessarily establish that a person is engaged in "other clandestine intelligence activity." Americans, through ignorance or inadvertence, may well technically violate campaign law requirements or foreign agent registration requirements, but to satisfy the requirements of the definition, it is necessary to show, separately from the criminal violation, probable cause to believe that the person is knowingly engaged in any other clandestine intelligence activities for or on behalf of such foreign power, *pursuant to the direction of an intelligence service or network of a foreign power.*

§ 101(b)(2)(C) -- Sabotage or Terrorism

Subsection 101(b)(2)(C) allows electronic surveillance or physical search of any person, including a U.S. person, who knowingly engages in sabotage or international terrorism, or activities in preparation therefor, for or on behalf of a foreign power. The terms "sabotage" and "international terrorism" are defined separately and require a showing of criminal activity. Mere sympathy for, identity of interest with or vocal support for the goals of a foreign group, even a foreign-based terrorist group, is not sufficient to justify surveillance under this subparagraph. The term "activities that are in preparation [for]" sabotage or international terrorism is intended to encompass activities supportive of acts of serious violence -- for example, purchase or surreptitious importation into the United States of explosives, planning for assassinations or financing of or training for such activities. Other activities supportive of terrorist acts could likewise satisfy this standard. The circumstances must be such as would lead a reasonable person to conclude that the subject is knowingly engaged in activities that are in preparation for sabotage or terrorism.

The term "preparation" does not mean preparation for a specific terrorist act. Because the definition of "international terrorism" speaks of a range of acts, and "preparation" as used here takes its meaning from the context of the definition of "international terrorism," it could reasonably be interpreted to include, *e.g.*, providing the personnel, training, funding or other means for the commission of acts of terrorism, rather than participating in a particular bombing. This provision also permits electronic surveillance or physical search at a time *before* the danger sought to be prevented -- whether a kidnaping, bombing or hijacking -- actually occurs.

The "preparation" standard allows surveillance where the government cannot establish that an individual has already knowingly engaged in an act of sabotage or terrorism, but there are sufficient specific and articulable facts to indicate that his activities are in preparation for such acts. The circumstances must be such as would lead a reasonable person to conclude that the subject is knowingly engaged in activities that are in preparation for sabotage or terrorism.

It should be noted that the "preparation" standard need apply only where there is insufficient information to show that the subject is, in fact, a terrorist. Where the FBI can show that the subject is a known international terrorist, such as the notorious "Carlos," or that he has been engaging in international terrorism for or on behalf of a group engaged in international terrorism, there is no need to show that he is in the act of preparing for further terrorist acts. In some cases, immediate arrest may not be possible, such as situations in which the subject may not have violated U.S. law, even though he may have murdered hundreds of persons abroad. In other cases it may be more fruitful to monitor the subject's activities in the United States to identify otherwise unknown terrorists located here, their international support structure and the locations of weapons or explosives. If a person who has engaged in international terrorism visits the U.S. or resides in the U.S., the FBI should be able to utilize electronic surveillance to monitor his activities, whether or not there is information showing that he is presently

70

planning some particular violent act.

Finally, a subject targeted for surveillance under this definition must be shown to have a knowing connection with the foreign power for whom he is working. In most cases of international terrorism, this connection will be shown to exist with a group engaged in international terrorism. The case may arise in which a U.S. person is acting for or on behalf of such a group that is substantially composed of U.S. persons. In such a case, the Court must examine the circumstances carefully in order to determine whether the organization is "a group engaged in international terrorism," as defined, and not a purely domestic group engaged in domestic terrorism. [Domestic terrorism is handled under criminal law processes, *e.g.*, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Title 18, U.S. Code, chapter 119, and the AG Guidelines for General Crimes.]

§101(b)(2)(D) -- Entering the U.S. under a False or Fraudulent Identity

This definition includes any person who knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power. The most obvious example would be the "illegal" who enters the United States under an assumed name and using a "legend" based on the vital statistics of a real person, usually dead. It would also include a person who enters the United States lawfully, then assumes a false identity, provided assuming such a false identity is done for or on behalf of a foreign power.

§101(b)(2)(E) -- Aiding, Abetting and Conspiracy

This definition includes any person, including a U.S. person, who knowingly aids or abets any person in the conduct of activities described in the preceding subsections, or knowingly conspires with any person to engage in such activities. The knowledge requirement is applicable to both the status of the person being aided and the nature of the activity being promoted. This means the FBI must establish probable cause to believe that the subject knows both that the person with whom he is conspiring or whom he is aiding or abetting is engaged in the described activities as an agent of a foreign power and that his own conduct is assisting or furthering such activities. The innocent dupe who unwittingly aids a foreign intelligence officer cannot be targeted under this provision.

In the case of a subject believed to be aiding or abetting persons engaged in international terrorism, the subject might be assisting a group engaged in both lawful political activity and unlawful terrorist acts. In such a case, it would be necessary to establish probable cause to believe that he was aware of the terrorist activities undertaken by the group and was knowingly furthering them, not merely that he was aware of and furthering the group's lawful activity.

Verification Procedures

[redacted]

b5-1
b2-2 b7E-1

[redacted]

FISA Court's Rule 11

By order dated May 17, 2002, the FISA Court promulgated "Rule 11, Criminal Investigations in FISA Cases":

> All FISA applications shall include informative descriptions of any ongoing criminal investigations of FISA targets, as well as the substance of any consultations between the FBI and criminal prosecutors at the Department of Justice or a United States Attorney's Office.

Rule 11 formalizes the requirement for descriptions of any ongoing criminal investigation, an issue that was addressed in the "verification procedures" dated April 5, 2001. Then Rule 11 adds the requirement to describe the substance of any consultations between the FBI and criminal prosecutors at DOJ or a United States Attorney's Office. The scope and degree of such consultations have proliferated significantly since promulgation of the AG's memo on information sharing on March 6, 2002, and access by prosecutors to intelligence information and to case files on intelligence investigations has reached unprecedented proportions [redacted]

b5-1 b2 b7E-1

72

[redacted]

b5-1
b2-b7E-1

73

[redacted]

Certification

Subsection 104(a)(7) of FISA requires a certification by the Assistant to the President for National Security Affairs -- or other Executive Branch official designated by the President from among those officials employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate. The designated presidential advisor is the only one specifically provided for in the statute. By Executive Orders 12139 and 12949 the President has also designated the Director (and Deputy) of Central Intelligence, the Secretary (and Deputy) of Defense, the Secretary (and Deputy) of State and the Director of the FBI. Note that the Deputy Director of the FBI is conspicuously absent -- the Deputy Director is typically a career Special Agent rather than an official appointed by the President with the advice and consent of the Senate and therefore does not meet the statutory prerequisites.

Foreign Intelligence Information

The certification consists of five elements, the first of which is that the official making the certification deems the information sought to be foreign intelligence information. If you relate these officials and their functions to the definition of "foreign intelligence information" in section 101(e) of the statute, there is a certain attraction of logic in their selection. Under subsection 101(e)(1), "foreign intelligence information" means information that relates to [or, if concerning a United States person, is *necessary* to] the ability of the United States to protect against (a) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (b) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (c) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power. These elements go to the classic counterintelligence and counterterrorism functions of the CIA and the FBI.

Under subsection 101(e)(2), the definition of "foreign intelligence information" includes information with respect to a foreign power or foreign territory that relates to [or, if concerning a United States person, is *necessary* to] (a) the national defense or the security or (B) the conduct of the foreign affairs of the United States. These elements implicate the missions and functions of the Secretary of Defense and the Secretary of State.

Under the scheme set up by Executive Order 12333, the Assistant to the President for National Security Affairs (the "National Security Advisor") is the senior Executive Branch official in the Intelligence Community and has interests in *all* of these matters.

The requirement that the certifier deems the information sought to be "foreign intelligence information" is designed to ensure that a senior official with responsibilities in the area of national security reviews the determination made at lower levels of the Executive Branch that the information sought is foreign intelligence information. The intent of FISA is ensure that the certifier carefully considers the substance of cases before him and does not simply sign off on boilerplate language. This prevents targeting a foreign power for electronic surveillance when the true purpose is to gather information about an individual for other than foreign intelligence purposes. It is also designed to make explicit that a significant purpose of such surveillance is to obtain "foreign intelligence information" as defined, rather than some other type of information. The certifier similarly must explain in his affidavit why the information cannot be obtained through less intrusive techniques. This requirement is particularly important when U.S. persons are the targets of surveillance or search.

A Significant Purpose

b5-1
b2, b7E-1
2

74

The second element of the certification is that "a significant purpose" of the surveillance or search is to obtain foreign intelligence information. Since the objective in enacting the statute is to provide a statutory procedure for the government to obtain a judicial order for electronic surveillance or physical search for foreign intelligence purposes, the "purpose" aspect of the certification is extremely important. The majority of pre-FISA caselaw had recognized a "national security exception" to the warrant requirement of the Fourth Amendment. In determining whether the cases before them should be accorded that exception, the courts tended to focus on whether the collection of foreign intelligence information was the "primary" purpose of the surveillance. In the case of *Humphrey and Truong* the trial judge concluded that the fruits of electronic surveillance and physical searches conducted without a warrant were admissible under the Fourth Amendment, provided those surveillances and searches had been conducted for a foreign intelligence purpose. The measure by which he determined purpose was direction and control of the surveillance, or investigation. So long as special agents of the FBI who normally investigated intelligence activities were directing and controlling the investigation, he construed the information as having been obtained for a foreign intelligence purpose. Conversely, when DOJ prosecutors began to write prosecutive memoranda and to control the direction of the investigation, he concluded that the information had been obtained for the purpose of prosecution and, accordingly, was inadmissible since it had been obtained without a warrant.

When FISA was enacted, it required that "the purpose" of the surveillance be to obtain foreign intelligence information. Based on experience with pre-FISA caselaw, the government's practice before the Foreign Intelligence Surveillance Court has been to construe "the purpose" as "primary purpose" and to determine purpose by following a procedure similar to that adopted in *Humphrey and Truong*. A reading of the legislative history of FISA suggests that subsection 104(a)(7) was intended to replace the *Humphrey-Truong* test with the accountable official's certification that the purpose of the surveillance or search is to acquire foreign intelligence information, as defined. The USA PATRIOT Act amended FISA to require that obtaining foreign intelligence information be a "significant" purpose of the surveillance or search. While there is a dearth of legislative history of this amendment, it would appear that the Congress intended to rectify perceived lapses in the government's handling of certain counterintelligence investigations with regard to the determination of probable cause to believe that he was an agent of a foreign power and to steer the government -- as well as the Foreign Intelligence Surveillance Court -- toward the statutory scheme of relying on the certification for determining purpose.

The information required by the FISC's Rule 11 is largely a recitation of criminal justice pursuits and appears to follow the pre-enactment practice of determining purpose through an examination of direction and control of the investigation. The Court's position in this regard was reiterated in its opinions of April 22 and May 17, 2002, regarding the AG's March 6, 2002, memo on information sharing. The certification required by subsection 104(a)(7) is not so much an analysis of direction and control as an affirmation of the intelligence objectives of the surveillance or search. The point for field agents to understand is that in submitting a request for initiation of FISA surveillance or search, it is important to articulate the specific intelligence objectives of the requested FISA coverage. *E.g.*, in an espionage case, those objectives might include identification of a subject's handler, or his tradecraft in servicing dead-drops or how he obtains access to classified information. In the case of a terrorism subject, the objectives of the surveillance might be to learn the extent of the subject's relationship with an international terrorist group. To ensure that the Director has a proper basis for making this certification, NSLU recommends that any communication to HQ requesting application to the Court for authorization to use a FISA technique should both articulate the intelligence objectives to be achieved through the use of FISA techniques and, to satisfy requirements imposed by the Court, describe any criminal aspect of the investigation in sufficient detail to determine that intelligence officials and not law enforcement officials are directing and controlling the use of FISA techniques.

Not Reasonably Obtainable by Other Means

The third element of the certification is that the information sought cannot reasonably be obtained by normal investigative techniques. There is not much legislative guidance on this requirement, but, in general terms, it appears to is based on the general principle -- subsequently reiterated in Executive Order 12333 -- that the Intelligence Community should respect individual privacy rights by conducting intelligence activities using the least intrusive techniques feasible. Thus, it would appear that, due to their intrusiveness, Congress intended FISA techniques should be a last -- rather than first -- resort. In most instances, this requirement can be satisfied by the fact that only surveillance or search of the kind authorized pursuant to FISA can adequately obtain the information sought. For example, if more visible or detectable means of surveillance were utilized, the subject would likely change his means of communication to something less susceptible of surveillance.

Category of Foreign Intelligence Information Sought

The fourth aspect of the certification is designation of the type of foreign intelligence information being sought according to the categories described in section 101(e) of the statute, whether one of the kinds of counterintelligence information defined in subsection 101(e)(1), or of positive intelligence as defined in subsection 101(e)(2).

Basis for Certification

The final part of the certification is a statement of the basis for the certification as to the third and fourth elements, *i.e.*, that the information sought is the type of foreign intelligence information designated, and that such information cannot reasonably be obtained by normal investigative techniques. Usually this is based on the results of the FBI's investigation to date. A presentation of facts relevant to this issue might follow a logical flow of relating the activities of the target that make him an "agent of a foreign power" as defined in subsection 101(b) to the appropriate definition of "foreign intelligence information" in subsection 101(e), coupled with a discussion of the technique that would be necessary to obtain that kind of intelligence information. This element of the certification is not required when the target of the electronic surveillance is a foreign power as defined in subsection 801(a)(1), (2) or (3), *i.e.*, a foreign government or component thereof; a faction of a foreign nation not substantially composed of United States persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.

Duration

The general rule is that the FISC may approve electronic surveillance for the period necessary to achieve its purpose, or for 90 days, whichever is less. There are certain exceptions. Electronic surveillance of a foreign power as defined in section 101(a)(1), (2) or (3) may be authorized for up to one year. Electronic surveillance of a foreign agent as defined in section 101(b)(1)(A) may be for the period specified in the application or for 120 days, whichever is less. Upon renewal, surveillance of a 101(b)(1)(A) agent of a foreign power may be for a period not to exceed one year.

An order authorizing physical search may be approved for the period necessary to achieve its purpose, or for 90 days, whichever is less. As with electronic surveillance, there are exceptions. Physical search of a foreign power, as defined in 101(a)(1), (2) or (3), may be authorized for the period specified in the application or for one year, whichever is less, and physical search of a section 101(b)(1)(A) agent of a foreign power may be authorized for the period specified in the application or for 120 days, whichever is less. An extension may be granted for a period not to exceed one year if the judge finds probable cause to believe that no property of any individual United States person will be acquired during the period in which search is authorized.

It is important to ensure that surveillance or searches adhere to the timelines specified in the orders. For one thing, the length of time involved in drafting a FISA application and preparing it for presentation to the Court requires that requests for renewal be forwarded in timely fashion. You cannot wait until two weeks before an order expires to submit a request for the next one. It is also imperative that actual surveillance or search not occur beyond the period of authorization specified in the order. If surveillance should overrun the period of authorization, any unauthorized "take" must be sequestered and forwarded to the Office of Intelligence Policy and Review, via the substantive unit at FBIHQ, for submission to the Foreign Intelligence Surveillance Court. The overrun must also be reported by electronic communication to the Inspection Management Unit of the Inspection Division within 14 days of discovery of the error. [See section 2-56.E of the National Foreign Intelligence Program Manual.]

Miscellaneous Considerations

Getting an order from the Court is only the beginning of the successful administration of the authorities granted pursuant to FISA. Among the practical considerations that should attend implementation of a FISA order is ensuring that the "premises" being surveilled are those named in the order. For example, it is important to ensure that telephone coverage is on the right telephone line. Clues that something is amiss might include the fact that intercepted communications are in a language other than that expected. Or the information obtained might appear to be non-pertinent to the intelligence objectives of the surveillance.

76

In cases of physical search, the Court typically requires a ... by the federal officer executing the search. The return is essentially a report to the Court of the circumstances under which the search was conducted and the information or tangible items seized. It is common for the Court to require a return within twenty-one (21) days of the execution of a search, but 21 days is not necessarily applicable to all cases, so it is important to note the specific requirements of individual orders.

Another practical consideration is the provision of subsection 105(c)(2) that the Court may order a communications common carrier, landlord, custodian or other specified person to furnish the applicant [the FBI] with all information, facilities or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy. In addition, the Court may order such persons maintain any records concerning the surveillance or the aid furnished that such person wishes to retain under security procedures approved by the Attorney General and the Director of Central Intelligence. Subsection 304(c)(2) makes similar provision for physical searches.

A recurring problem is service of the order on service providers or other specified persons who lack security clearances or, in some cases, the wherewithal to store classified orders properly. When FISA was originally enacted, the overwhelming bulk of the surveillance was simple telephone wiretaps, and there were only a few large communications common carriers with which to deal. As a result, it was relatively easy to obtain clearances for a security office at a large carrier to obtain proper access to information and storage facilities. Since then, however, the large telephone companies have broken up into numerous "baby bells," leading to a proliferation of the workload involved with background investigations and clearances. In addition, the advent of the Internet and the concomitant proliferation of Internet service providers have also added to investigative and security clearance workloads.

The security procedures approved by the Attorney General and the Director of Central Intelligence empower the SAC to authorize disclosure of a classified order on an emergency basis under circumstances in which such disclosure is necessary to execute the order. As a rule, the classified information contained in a secondary order is typically limited to identification of the target -- which information is frequently communicated to the service provider anyway in preliminary discussion. As a result, showing a service provider the secondary order typically amounts to disclosure of something he already knows -- the identity of the subject of surveillance. In a case in which an ongoing relationship is not likely and there is no need for the service provider to have longterm access to classified information, the SAC may authorize showing the secondary order to a service provider or other specified person on a one-time basis. It is recommended that the service provider be offered a "trust receipt" that relates back to the order by date and docket number and that the field office secure the secondary order. The service provider should be advised that the order will be made available should the need arise. If needed, a copy of the security procedures [which are classified] and a model trust receipt may be obtained from NSLU via Groupwise e-mail.

With regard to the trust receipt, the most common concern expressed by service providers is the fear of being sued for providing assistance to the FBI. Service providers may be advised of the following provision of subsection 105(i):

> No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act for electronic surveillance or physical search.

In addition to this statutory protection from civil liability, if a service provider were to be sued for assisting the FBI in conducting electronic surveillance or physical search pursuant to FISA, the Bureau would seek the Attorney General's assertion of the State Secrets Privilege [*United States v. Reynolds*, 345 U.S. 1 (1953)] to prevent the disclosure of classified information that would be required to sustain such a cause of action. If a field office is contacted by a service provider about such a situation, NSLU should be notified immediately.

Coming Attractions . . .

The gathering of information, including information as to the capabilities, intentions and activities of foreign powers and their agents, would be meaningless without successful exploitation of that information to protect the

77

United States from hostile attack and other grave acts, acts of terrorism, sabotage and clandestine intelligence activities. Bearing in mind that the recurring theme in various provisions of FISA is the balancing of individual rights to privacy against the need of the government's need to acquire and produce foreign intelligence information, FISA creates a heavy burden with regard to managing the acquisition, retention and dissemination of U.S. person information. In sum, this is the process of "minimization." As most minimization procedures are classified, minimization is not addressed here in detail. In addition, the procedures for "information sharing" promulgated by the Attorney General on March 6 and modified somewhat by the FISA Court are still subject to judicial review. Accordingly, procedures for the sharing of information will be the subject of a separate communication.

Top of Page

Last Updated: Thursday, September 12, 2002

78

EXHIBIT III

STORED WIRE & ELECTRONIC COMMUNICATIONS QUICK REFERENCE GUIDE

(REFLECTING 2001 UPDATES FROM P.L. 107-56, USA PATRIOT ACT)

	Voluntary Disclosure Allowed?		Mechanisms to Compel Disclosure	
	Public Provider	**Non-Public Provider**	**Public Provider**	**Non-Public Provider**
Basic subscriber, session & billing information†	No, unless §2702(c) exception applies [§ 2702(a)(3)]	Yes [§ 2702(a)(3)]	Subpoena; 2703(d) order; or search warrant [§ 2703(c)(2)]	Subpoena; 2703(d) order; or search warrant [§ 2703(c)(2)] [§ 2711(2)]
Other transactional and account records	No, unless §2702(c) exception applies [§ 2702(a)(3)]	Yes [§ 2702(a)(3)]	2703(d) order or search warrant [§ 2703(c)(1)]	2703(d) order or search warrant [§ 2703(c)(1)]
Retrieved communications‡ and content of other stored files	No, unless § 2702(b) exception applies [§ 2702(a)(2)]	Yes [§ 2702(a)(2) and § 2711(2)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(b)]	Subpoena; ECPA doesn't apply [§ 2711(2)]
Unretrieved communications‡ (in electronic storage more than 180 days)	No, unless § 2702(b) exception applies [§ 2702(a)(1)]	Yes [§ 2702(a)(1)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(a,b)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(a,b)]
Unretrieved communications‡ (in electronic storage 180 days or less)	No, unless § 2702(b) exception applies [§ 2702(a)(1)]	Yes [§ 2702(a)(1)]	Search warrant [§ 2703(a)]	Search warrant [§ 2703(a)]

† See 18 U.S.C. § 2703(c)(2) for listing of information covered. For telephone communications, the section includes, among other records, local and long distance connection records. For Internet connections, the section includes, among others, records of session times and durations, and IP address assigned to the user during the session.

‡ Includes the content of voice communications.

Computer Crime and Intellectual Property Section ✩ United States Department of Justice
P.O. Box 887 ✩ Ben Franklin Station ✩ Washington, D.C. 20044-0887
Main (202) 514-1026 ✩ Fax (202) 514-6113 ✩ www.cybercrime.gov

EXHIBIT IV

Exemption (b)(1) Narratives

DESCRIPTION OF DOCUMENT CONTAINING NATIONAL SECURITY INFORMATION

Exhibit: I; Page Numbers: 1 and 2

Subject: FISA

Date of Document: 2/4/2003

Total Number of Pages: 2

Total Number of Pages Containing National Security Information: 2

Description of Document: FISA Report

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions on **page 1** and on **page 2**, (**pages 1 and 2**). The information withheld is a listing of Court authorized FISAs active within a specific time frame. The list identifies the specific target of each FISA; the file number assigned to each Foreign Counterintelligence/International Terrorism (FCI/IT)investigation involving the FISA; the specific field office or office of origin where the investigation is on-going; the authorization and expiration dates of each listed FISA; and the total number of FISAs.

The FBI conducts FCI/IT investigations to determine whether a foreign intelligence officer or agent or international terrorist group is seeking to infiltrate an organization in order to influence or control it. In addition, FCI/IT investigations are conducted to determine whether an organization or group substantially composed of U.S. persons (citizen or resident aliens) is acting for or on behalf of a foreign power. Disclosure of a target or of the existence of the FISA would reveal the FBI's intelligence activity and method.

A file number that is assigned to a specific intelligence activity and identifies channelization/dissemination instructions for information identifiable with the intelligence activity. Individual file numbers are assigned by FBI Headquarters ("FBIHQ") and field offices and contain the geographical prefix or the originating office, and the case number, which includes the numerical characterization of the type of investigation followed by a chronological number indicating the number assigned to a specific investigation/activity. A disclosure of the intelligence activity file numbers can lead to the exposure of actual current intelligence activities or operations.

The office of origin is the FBI's field office that instituted the original investigation regarding the individual or organization of national security interest. Disclosure of this information could reveal the scope and thrust of the FBI's intelligence activities and methods directed at specific targets of national security interest within a specific time frame.

It is my determination that the release of any portion of the information classified and withheld in this document could reasonably be expected to cause serious damage to the national security, as it would: (1) reveal the existence, methodology, and time frame of the FBI counterintelligence activities directed at specific targets of national security interest (2) reveal the nature, objective, and requirements, and scope of a specific FBI counterintelligence activity or method; (3) disclose the intelligence-gathering capabilities of the activity or method and (4) provide an assessment of the intelligence source penetration during a specific period of time. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). <u>See</u> Second Declaration of Christine Kiefer ("Second Kiefer Declaration"), ¶¶

27-28.

DESCRIPTION OF DOCUMENT CONTAINING NATIONAL SECURITY INFORMATION

Exhibit: I; PAGE NUMBERS: 3 and 4

Subject: PEN REGISTERS SINCE 10/26/2001

Date of Document: 2/05/2003

Total Number of Pages: 2

Total Number of Pages Containing National Security Information: 2

Description of Document: Report listing the total number of Pen Registers issued since 10/26/2001

Justification of Deletions

The classified information withheld in this document is contained within the **bracketed portions** contained on **pages 1** and **2**, (**pages 3 and 4**). The withheld information identifies **project numbers**, which are numbers chronologically assigned to each request by the field offices to FBI Headquarters National Security Law Unit ("NSLU") for the issuance of a pen register and the "**Completed Date**", which is the completion date of the **pen register.** The withheld information also contains the total number of pen register's issued since 10/26/2001. The release of this information could reveal the scope and thrust of the FBI's intelligence activities and methods directed at specific targets of national security interest within a specific time frame.

It is my determination that the disclosure of this classified information could reasonably be expected to cause serious damage to the national security, as it would: (1) reveal the existence, methodology, and time frame of FBI counterintelligence activities directed at a specific targets of national security (2) reveal the nature, objective, requirements, and scope of a specific FBI counterintelligence activity, (3) disclose the intelligence-gathering capabilities of the activity, and (4) provide an assessment of the intelligence source penetration during a specific period of time. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities during a particular time frame, and an evaluation of hostile intelligence plans and programs that have or have not been compromised. This would allow hostile agents to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 5

Subject: Business Record Order Requests Since 10/26/2001

Date of Document: 2/07/03

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Report Listing the Number of FISA requests for Business Records since 10/26/2001.

Justification of Deletions

The classified information withheld in this document is contained within the **bracketed portions** of **page 1**. The withheld information identifies **project numbers (ProjID)**, which are numbers chronologically assigned to each FISA request from the field offices to the National Security Law Unit (NSLU) at FBI Headquarters, the date the NSLU received each request and the total number of requests received since 10/26/2001. The release of this information could reveal the scope and thrust of the FBI's intelligence activities and methods directed at specific targets of national security interest within a specific time frame.

It is my determination that the disclosure of this classified information could reasonably be expected to cause serious damage to the national security, as it would: (1) reveal the existence, methodology, and time frame of FBI counterintelligence activities directed at a specific targets of national security (2) reveal the nature, objective, requirements, and scope of a specific FBI counterintelligence activity, (3) disclose the intelligence-gathering capabilities of the activity, and (4) provide an assessment of the intelligence source penetration during a specific period of time. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities during a particular time frame, and an evaluation of hostile intelligence plans and programs that have or have not been compromised. This would allow hostile agents to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 30

Subject: Not Indicated

Date of Document: Not Indicated

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal Handwritten Note

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portion **below the handwritten notation "NSL'S-(#s from NSLU)"**. The information withheld identifies the total number of National Security Letters (NSL's) that where authorized within specific time periods. Disclosure of this information could reveal the scope and thrust of the FBI's intelligence activities and methods directed at specific targets of national security interest within a specific time frame.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) reveal the existence, methodology, and time frame of the FBI counterintelligence activities directed at specific targets of national security interest (2) reveal the nature, objective, and requirements, and scope of a specific FBI counterintelligence activity or method; (3) disclose the intelligence-gathering capabilities of the activity or method and (4) provide an assessment of the intelligence source penetration during a specific period of time. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). <u>See</u> Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 31

Subject: Congressional Briefing Re Patriot Act Provisions

Date of Document: 8/14/02 4:30PM

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal E-Mail

Justifications of Deletions

The classified information withheld in this document is contained within the bracketed portion of **lines 1-3** of **paragraph 1**. The information withheld identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's Minneapolis field office in its intelligence gathering operations. Disclosure of this information would identify specific activities and methods used by this field office and how aggressively they are being utilized.

It is my determination that release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 33

Subject: Patriot Act Feedback

Date of Document: 8/15/02 7:39PM

Total Number of Pages: 1

Total Number of Pages Containing
National Security Information: 1

Description of Document: Internal E-Mail

Justifications of Deletions

The classified information withheld in this document is contained within the bracketed portion of **lines 1-4** of **paragraph 2**. The information withheld identifies specific problems encountered by the FBI when utilizing a specific investigative tool authorized under the Patriot Act and its recommendations for amendment of Section 216. Disclosure of this information would identify specific activities and methods used by the FBI and how aggressively they are being utilized.

It is my determination that release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 37

Subject: USA Patriot Act

Date of Document: 6/17/2002 2:51PM

Total Number of Pages: 1

Total Number of Pages Containing
National Security Information: 1

Description of Document: Internal E-Mail

Justifications of Deletions

The classified information withheld in this document is contained within the bracketed portion of lines 1-5 of paragraph 2; the bracketed portions of lines 4 and 6 of paragraph 3; the bracketed portion of line 3 of paragraph 4; the bracketed portion of lines 1 and 2 of paragraph 5; and the bracketed portion of line 1 of paragraph 6. The information withheld identifies an individual or organization as the subject of an FBI national security investigation and identifies a specific investigatory tool authorized under the Patriot Act, which is currently being utilized by the FBI's Minneapolis field office, in its intelligence gathering operations targeting this subject. Disclosure of this information would reveal the target of the intelligence or counterintelligence investigation and the activities and methods directed at the target.

It is my determination that disclosure of this information could reasonably be expected to cause serious damage to the national security as it would: (1) reveal the FBI's ongoing national security investigation; (2) reveal the scope and depth of the FBI's intelligence activities and methods directed against the target; and (3) alert the target and other targets of possible intelligence investigations and allow them to take countermeasures to thwart the FBI's capabilities to monitor and retrieve intelligence information. This would disrupt the intelligence gathering process and severely hamper the FBI's efforts to detect and apprehend those who seek to damage the national security. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 39

Subject: Patriot Act response

Date of Document: 8/15/02 5:17PM

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions of **lines 1-7** of **paragraph 1**. The information withheld identifies specific investigatory tools authorized under the Patriot Act, which are currently being utilized and those which have yet to be utilized by a specific squad of the FBI's Los Angles field office in its intelligence gathering operations. The withheld information also details how a specific tool is being utilized by this squad to obtain intelligence or counterintelligence information. Disclosure of this information would identify specific activities and methods and how aggressively they are being utilized.

It is my determination that the release of this

information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 40

Subject: Patriot Act Provisions Which Need Further Examination

Date of Document: Not Indicated

Total Number of Pertinent Pages: 2

Total Number of Pages Containing National Security Information: 1

Description of Document: Report Summarizing possible Amendments to the Patriot Act

Justifications of Deletions

The classified information withheld in this document is contained within the bracketed portion of **lines 1 and 2** of **paragraph 6**. The information withheld contains standard terminology or phraseology which appears in the most recent FBI investigations. Disclosure will reveal the scope and depth of the FBI's investigation of a particular intelligence matter. Stated another way, disclosure will reveal the limitations of the FBI's efforts in a particular investigation or the amount of resources or efforts that the FBI is willing to expend on this particular matter. This allows a target to determine what information has been learned concerning him and what additional steps may be expected. If the information described by this phraseology is shallow, yet the subject was heavily involved in matters under investigation, it alerts the subject to the fact that his activities may continue without fear or detection. Conversely, if the information is substantial, it will prompt the subject to alter his course of conduct. Although these results may not occur in the narrow context of this case, the results described are likely to occur if information of this nature is routinely released.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security as it would reveal a specific intelligence activity or method. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 42

Subject: Patriot Act Provisions Which Need Further Examination

Date of Document: Not Indicated

Total Number of Pertinent Pages: 2

Total Number of Pages Containing National Security Information: 1

Description of Document: Report Summarizing possible Amendments to the Patriot Act

Justifications of Deletions

The classified information withheld in this document is contained on **page 1** within the bracketed portion of **lines 1-2** of **paragraph 6**. The withheld information is the same as previously addressed on **page 40**; therefore, the justifications for withholding this information are the same.

DESCRIPTION OF DOCUMENT CONTAINING NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 45

Subject: Briefing on the Patriot Act

Date of Document: 8/1/02 10:46AM

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained in **paragraph 2**, withheld in its entirety, under the sub-caption **"Usage"**. The information withheld identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's Kansas City field office in its intelligence gathering operations. The withheld information also indicates the number of times each tool has been utilized by this field office. Disclosure of this information would identify specific activities and methods and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities

to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromise an allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). <u>See</u> Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 46

Subject: Request for CDC assistance

Date of Document: 8/16/02 12:01PM

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions of **lines 2, 4 and 5** of **paragraph 2**. The information withheld identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's Little Rock field office in its intelligence gathering operations. Disclosure of this information would identify specific activities and methods used by this field office and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently

utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). <u>See</u> Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 47

Subject: Request for Assistance from the CDCs

Date of Document: 8/16/02 5:03PM

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions of **lines 1-3** of **paragraph 1**. The information withheld identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's Birmingham field office in its intelligence gathering operations. The withheld information also indicates the approximate number of times each tool has been utilized by this field office. Disclosure of this information would identify specific activities and methods used by this field office and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage

to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). <u>See</u> Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 49

Subject: Request for Assistance from the CDCs

Date of Document: 8/15/02 5:29PM

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portion of **line 1** of **paragraph 1**. The information withheld identifies a specific investigatory tool authorized under the Patriot Act, which has been or is currently being utilized by the FBI's Boston field office in its intelligence gathering operations. The withheld information also indicates the approximate number of times this tool has been utilized by this field office. Disclosure of this information would identify specific activities and methods used by this field office and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities

to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 51

Subject: Use of Patriot Act

Date of Document: 8/15/02 12:29PM

Total Number of Pages: 1

Total Number of Pages Containing
National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions of **lines 3-8** and **lines 14-18** below **paragraph 1**. The information withheld identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's Washington field office in its intelligence gathering operations. The withheld information also indicates the number of times each tool has been utilized by this field office. Disclosure of this information would identify specific activities and methods used by this field office and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage

to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromise an allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

Also, withheld specifically within the bracketed portions of **lines 3, 5, 6, 8, 14, 16** and **17** is the identity of investigative units of the Washington Field Office. The withheld units specialize in the investigation of specific intelligence cases or activities. Disclosure of these units, when combined with other known or disclosed information, could reasonably be expected to identify specific intelligence activities. It is my determination that the disclosure of the investigative unit withheld from release could reasonably be expected to cause serious damage to the national security, as it would reveal actual intelligence activities within a specific location. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 52

Subject: Re: Patriot Act

Date of Document: 8/15/02 3:04PM

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained in **paragraph 3**, withheld in its entirety. The information withheld identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's Omaha field office in its intelligence gathering operations. Disclosure of this information would identify specific activities and methods used by this field office and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently

utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromise an allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). <u>See</u> Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 53

Subject: Request for Assistance from the CDCs

Date of Document: 8/15/02 12:26PM

Total Number of Pages: 1

Total Number of Pages Containing
National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions of lines 2-5 of paragraph 1. The information withheld identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's Phoenix field office in its intelligence gathering operations. The withheld information also indicates the number of times each tool has been utilized by this field office. Disclosure of this information would identify specific activities and methods and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities

to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromise an allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 54

Subject: Patriot Act

Date of Document: 8/16/02 2:32PM

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions of **lines 3-5**; **11 and 12**; and **16-18** below **paragraph 1**. The information withheld identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's San Francisco field office in its intelligence gathering operations. The withheld information also indicates the number of times each tool has been utilized by this field office. Disclosure of this information would identify specific activities and methods used by this field office and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage

to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromise an allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 55

Subject: USA Patriot Act

Date of Document: 8/16/02 4:31PM

Total Number of Pages: 1

**Total Number of Pages Containing
National Security Information: 1**

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions of **lines 3-7** of the paragraph. The information withheld identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's Portland field office in its intelligence gathering operations. The withheld information also indicates the number of times each tool has been utilized by this field office. Disclosure of this information would identify specific activities and methods and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities

to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromise an allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 56

Subject: Investigative tools under the Patriot Act

Date of Document: 8/12/02 6:38PM

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions of **lines 1, 8 and 9** of **paragraph 1**. The information withheld identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's Sacramento field office in its intelligence gathering operations. The withheld information also indicates the approximate number of times each tool has been utilized by this field office. Disclosure of this information would identify specific activities and methods used by this field office and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage

to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Numbers: 58 and 59

Subject: Routing Slip and attachment dated 8/13/03

Date of Document: 8/15/02 4:38PM

Total Number of Pages: 2

Total Number of Pages Containing National Security Information: 2

Description of Document: FBI Memorandum

Justification of Deletions

The classified information withheld in this document is as follows:

Page 1, (page 58): The bracketed portion located in the **"From"** line contains the designated unit within the Miami field office which specializes in the investigation of specific intelligence cases or activities. Disclosure of the unit, when combined with other known or disclosed information, can reasonably be expected to identify the specific intelligence activity.

It is my determination that the disclosure of the investigative unit release could reasonably be expected to cause serious damage to the national security, as it would reveal actual intelligence activities within a specific location. See

Second Kiefer Declaration, ¶¶ 27-28.

The bracketed portions of **lines 1-4** of **paragraph 1** and **paragraphs 2 and 3**, withheld in their entirety, identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's Miami field office in its intelligence gathering operations. Disclosure of this information would identify specific activities and methods used and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

Page 2, (page 59): The bracketed portion of **line 1** located in the upper left margin contains the designated unit which specializes in the investigation of specific intelligence cases or activities. Disclosure of the unit, when combined with other known or disclosed information can reasonably be expected to identify the specific intelligence activity.

It is my determination that the disclosure of the investigative unit withheld from release could reasonably be expected to cause serious damage to the national security, as it would reveal actual intelligence activities within a specific location. See Second Kiefer Declaration, ¶¶ 27-28.

The bracketed portions of **lines 4, 5, 11 ,12 and 15** identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's Miami field office in its intelligence gathering operations. Disclosure of this information would identify specific activities and methods used and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). <u>See</u> Second Kiefer Declaration, ¶¶ 27-28.

**DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION**

Exhibit: I; Page Number: 68

Subject: Staff Brief re: Patriot Act

Date of Document: 8/8/02 2:11PM

Total Number of Pages: 1

**Total Number of Pages Containing
National Security Information: 1**

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions of **line 1** under the sub-caption **"Baltimore"** and **line 3** under the sub-caption **"Kansas City"**. The information withheld identifies a specific investigatory tool authorized under the Patriot Act, which has been or is currently being utilized by the FBI's Baltimore and Kansas City field offices in their intelligence gathering operations. The withheld information also indicates the number of times each tool has been utilized by each of these field offices. Disclosure of this information would identify specific activities and methods used by these field offices and how aggressively they are being utilized.

It is my determination that the release of this

information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 70

Subject: Patriot Act

Date of Document: 8/15/02 2:50PM

Total Number of Pages: 2

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained on **page 2**, in **paragraph 2**, which is withheld in its entirety. The information withheld identifies a specific investigatory tool authorized under the Patriot Act, which has been or is currently being utilized by the FBI's New Orleans field office in its intelligence gathering operations. Disclosure of this information would identify specific activities and methods used by this field office and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently

utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). <u>See</u> Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 71

Subject: Re: Request for Assistance from the CDCs

Date of Document: 8/16/02 10:15AM

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions of **lines 1-3** under the sub-caption **"Albany Division"**. The information withheld identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's Albany field office in its intelligence gathering operations. The withheld information also indicates the number of times each tool has been utilized by this field office. Disclosure of this information would identify specific activities and methods used by this field office and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage

to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromise an allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

In addition, the withheld information contained within the brackets in the **lower left portion** of the document contains a handwritten notation which identifies a specific investigatory tool authorized under the Patriot Act, which has been or is currently being utilized by the FBI's field offices in their intelligence gathering operations. The withheld information also indicates the total number of times this specific tool has been utilized by field offices during a specific time frame. Disclosure of this information would identify specific activities and methods used by the field offices and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromise an allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 72

Subject: Re: CDC Request re Patriot Act Enhancements

Date of Document: 8/19/02 2:53PM

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained in **paragraph 5**, withheld in its entirety. The information withheld identifies a specific investigatory tool authorized under the Patriot Act, which has been or is currently being utilized by the FBI's Norfolk field office in its intelligence gathering operations. Disclosure of this information would identify specific activities and methods used by this field office and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently

utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromise an allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 73

Subject: Request for Assistance from the CDCs

Date of Document: 8/15/02 4:56PM

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions of **lines 3** and **4** of **paragraph 1**. The information withheld identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's Atlanta field office in its intelligence gathering operations. Disclosure of this information would identify specific activities and methods used by this field office and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently

utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). <u>See</u> Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING
NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 75

Subject: Request for Assistance from the CDCs

Date of Document: 8/16/02 2:03PM

Total Number of Pages: 1

Total Number of Pages Containing
National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions of lines 1-3 of paragraph 1. The information withheld identifies a specific investigatory tool authorized under the Patriot Act, which has been or is currently being utilized by the FBI's Honolulu field office in its intelligence gathering operations. The withheld information also indicates the frequency this tool has been utilized by this field office. Disclosure of this information would identify specific activities and methods used by this field office and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities

to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromise an allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 76

Subject: Staff Brief re: Patriot Act

Date of Document: 8/8/02 2:23PM

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions of **line 1** under the sub-caption **"Baltimore"** and line 3 under the sub-caption **"Kansas City"**. The information withheld identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's Baltimore and Kansas City field offices in their intelligence gathering operations. The withheld information also indicates the number of times each tool has been utilized by each of these field offices. Disclosure of this information would identify specific activities and methods used by these field offices and how aggressively they are being utilized.

It is my determination that the release of this

information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). <u>See</u> Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 77

Subject: PUBLIC LAW 107-56-OCT. 26,2001

Date of Document: 8/21/02

Total Number of Pages: 2

Total Number of Pages Containing National Security Information: 1

Description of Document: Table of content from the USA Patriot Act of 2001

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions of the **lower left margin** and the **lower right margin**. The withheld information indicates the approximate number of times each investigatory tool authorized under the Patriot Act has been utilized by the FBI in its intelligence gathering operations. Disclosure of this information would identify specific activities and methods and how aggressively they are being utilized.

It is my determination that the release of this information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). <u>See</u> Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING NATIONAL SECURITY INFORMATION

Exhibit: I; Page Number: 79

Subject: Fwd: Message to all CDCs/ADCs

Date of Document: 8/13/02 4:29PM

Total Number of Pages: 1

Total Number of Pages Containing National Security Information: 1

Description of Document: Internal E-mail

Justification of Deletions

The classified information withheld in this document is contained within **paragraphs 2, 4,and 6**, withheld in their entirety, and the bracketed portions of **lines 1 and 3** of **paragraph 7**. The information withheld identifies specific investigatory tools authorized under the Patriot Act, which have been or are currently being utilized by the FBI's Jacksonville field office in its intelligence gathering operations. The withheld information also indicates the approximate number of times each tool has been utilized by this field office. Disclosure of this information would identify specific activities and methods used by this field office and how aggressively they are being utilized.

It is my determination that the release of this

information could reasonably be expected to cause serious damage to the national security, as it would: (1) allow hostile entities to discover what activities or methods the FBI is currently utilizing in its intelligence or counterintelligence gathering operations; (2) reveal the nature, objective, and requirements, of a specific FBI counterintelligence activity or method; and (3) disclose the intelligence-gathering capabilities of the activity or method. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities within specific areas and during a particular time frame. This would provide hostile agents with an evaluation of hostile intelligence plans and programs that have or have not been compromised and allow them to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). <u>See</u> Second Kiefer Declaration, ¶¶ 27-28.

DESCRIPTION OF DOCUMENT CONTAINING NATIONAL SECURITY INFORMATION

Exhibit: II; Page Numbers: 38-43

Subject: Transactional Records NSLs Since 10/26/2001

Date of Document: Tuesday, January 21, 2003

Total Number of Pages: 6

Total Number of Pages Containing National Security Information: 6

Description of Document: Computer generated report

Justification of Deletions

The classified information withheld in this document is contained within the bracketed portions of **pages 1-6**. The withheld information identifies **project numbers**, which are numbers chronologically assigned to each request to FBI Headquarters for the issuance of a National Security Letter ("NSL"),and the date FBI Headquarters approved and issued the NSL. The release of this information could reveal the scope and thrust of the FBI's intelligence activities and methods directed at specific targets of national security interest within a specific time.

It is my determination that the disclosure of this classified information could reasonably be expected to cause serious damage to the national security, as it would:

(1) reveal the existence, methodology, and time frame of FBI counterintelligence activities directed at specific targets of national security interest; (2) reveal the nature, objective, requirements, and scope of a specific FBI counterintelligence activity; (3) disclose the intelligence-gathering capabilities of the activity; and (4) provide an assessment of the intelligence source penetration during a specific period of time. The release of this information could permit hostile governments to accurately evaluate the FBI's counterintelligence capabilities during a particular time frame, and an evaluation of hostile intelligence plans and programs that have or have not been compromised. This would allow hostile agents to devise countermeasures to circumvent these intelligence activities and render them useless in providing intelligence information, as well as make present and prospective U.S. counterintelligence operations more difficult if not impossible. This would severely disrupt the FBI's intelligence gathering capabilities and adversely impact the national defense. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 12,958, Section 1.5 (c). See Second Kiefer Declaration, ¶¶ 27-28.