U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

MS. MARCIA HOFMANN
ELECTRONIC FRONTIER FOUNDATION
SUITE 650
1875 CONNECTICUT AVENUE, N.W.
WASHINGTON, DC 20009

July 5, 2007

Subject: NATIONAL SECURITY LETTERS/USE

FOIPA No. 1073946- 000

Dear Ms. Hofmann:

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) Rule 6(e), Federal Rules of Criminal Procedure (FRCP)	☒(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)

1502 **page(s)** were reviewed and 1138 **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 Director, Office of Information and Privacy, U.S. Department of Justice,1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001 within sixty days from the date 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
Record/Information
Dissemination Section
Records Management Division

Enclosure(s)

Enclosed is the first interim release of documents. Set forth below is a list of the documents being released with this letter:

263-O-U-volume 8
263-O-U-volume 10
263-O-U-volume 14
263-O-U-volume 17
263-O-U-volume 18
263-O-U-volume 20
263-O-U-volume 22
263-O-U-volume 23
CTD-section 1
CTD-CD-volume 1
CTD-CD-volume 15
CTD-CD-volume 16
CTD-CD-volume 17
CTD-CD-volume 18
CTD-CD-volume 20
CTD-CD-volume 21
CTD-CD-volume 22
CTD-CD-volume 23
CTD-CD-volume 24
CTD-CD-volume 25
CTD-CD-volume 26
CTD-CD-volume 27
OIG-Exigent Letters/2005 # 1
OIG-Exigent Letters/2003 # 2
Model Letters et. al.
OIG-Data-NSL-Usage-volume 18

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could be reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could be reasonably expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

Freedom of Information and Privacy Acts

SUBJECT: NATIONAL SECURITY LETTERS
FOLDER: MODEL LETTERS ET AL

Federal Bureau of Investigation

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ COVER SHEET 05/02/2007

Total Deleted Page(s) ~ 1
Page 4 ~ b2, b7E

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

[DRAFTING DIVISION]
[STREET ADDRESS]
[CITY, STATE, ZIP CODE]
[MONTH, DAY, YEAR]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-07-2007 BY 65179/DMH/KSR/RW

1076786

[MR./MRS./MS.] [COMPLETE NAME OF POC]
[TITLE, IF AVAILABLE]
[NAME OF COMPANY]
[PHYSICAL STREET ADDRESS - NO P.O. BOX]
[CITY, STATE - NO ZIP CODE]

DEAR [MR./MRS./MS.] [LAST NAME]:

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (section 201 of the Electronic Communications Privacy Act, as amended), you are hereby directed to provide the Federal Bureau of Investigation (FBI) the names, addresses, and length of service and electronic communications transactional records, to include existing transaction/activity logs and all electronic mail (e-mail) header information (not to include message content and/or subject fields), for the below-listed **[e-mail/IP]** address holder(s):

[E-mail/IP ADDRESS or ADDRESSES]

[ON A SPECIFIC DATE]

or

[FOR THE PERIOD FROM [SPECIFIC DATE] TO [SPECIFIC DATE]
or [PRESENT]]

Please see the attachment following this letter for the types of information that you might consider to be a electronic communications transactional record.

If the time period noted above is to the "present," that term is intended to direct production of information to the date of the processing of this letter. If providing information to the date of processing is not feasible, please provide information to the date of receipt of this letter.

While fulfilling your obligations under this letter, please do not disable, suspend, lock, cancel or interrupt service to the above-described subscriber(s) or accounts. A service interruption or degradation may alert the subscriber(s)/account

users(s) that investigative action is being taken. If you are not able to fulfill your obligations under this letter without alerting the subscriber/account user, please contact the FBI prior to proceeding.

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

[Certification: The nondisclosure requirement is not an automatic feature of the NSL. If the supporting EC for this NSL included Option 1 (Invoking the Nondisclosure Requirement), then include the language in the following 3 paragraphs in the NSL.]

In accordance with 18 U.S.C. § 2709(c)(1), I certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person. Accordingly, 18 U.S.C. § 2709(c)(1) and (2) prohibits you, or any officer, employee, or agent of yours, from disclosing this letter, other than to those to whom disclosure is necessary to comply with the letter or to an attorney to obtain legal advice or legal assistance with respect to this letter.

In accordance with 18 U.S.C. § 2709(c)(3), you are directed to notify any persons to whom you have disclosed this letter that they are also subject to the nondisclosure requirement and are therefore also prohibited from disclosing the letter to anyone else.

In accordance with 18 U.S.C. § 2709(c)(4), if the FBI asks for the information, you should identify any person to whom such disclosure has been made or to whom such disclosure will be made. In no instance will you be required to identify any attorney to whom disclosure was made or will be made in order to obtain legal advice or legal assistance with respect to this letter.

[Include the following language in all NSLs.]

In accordance with 18 U.S.C. § 3511(a) and (b)(1), you have a right to challenge this letter if compliance would be unreasonable, oppressive, or otherwise unlawful, and you have the

right to challenge the nondisclosure requirement, if set forth above.

In accordance with 18 U.S.C. § 3511(c), an unlawful failure to comply with this letter, including any nondisclosure requirement, may result in the United States bringing an enforcement action.

You are directed to provide records responsive to this letter **[personally to a representative of the [DELIVERING DIVISION]** OR **through use of a delivery service to [OFFICE OF ORIGIN]** OR **through secure fax]** within [xxxx] business days of receipt of this letter.

Any questions you have regarding this letter should be directed only to the **[[DELIVERING DIVISION]** OR **[OFFICE OF ORIGIN],_depending on whether service is personal or through a delivery service].** Due to security considerations, you should neither send the records through routine mail service nor non-secure fax, nor disclose the substance of this letter in any telephone conversation.

Your cooperation in this matter is greatly appreciated.

Sincerely,

[ADIC/SAC NAME]

**[ASSISTANT DIRECTOR IN CHARGE/
SPECIAL AGENT IN CHARGE]**

(Rev. 08-28-2000)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date: 00/00/2007**

To: General Counsel **Attn:** Julie Thomas
Deputy General Counsel, NSLB

[COUNTERTERRORISM/ COUNTERINTELLIGENCE/CYBER] **Attn: [UNIT]**

[REQUESTING OFFICE] **Attn:** SSA **[SQUAD SUPERVISOR]**
SA **[CASE AGENT]**

[OFFICE OF ORIGIN] **Attn:** SA **[CASE AGENT]**
[Squad] [X]

[DELIVERING DIVISION] **Attn:** SSA **[SQUAD SUPERVISOR]**
(if using personal service) **[Squad] [X]**

From: [DRAFTING DIVISION]
[APPROVING OFFICIAL]
Contact: [CASE AGENT, telephone number (000)000-0000]

Approved By: **[ADIC NAME (IF APPLICABLE)]**
[SAC NAME]
[ASAC NAME]
[CDC NAME]
[SSA NAME]

DECLASSIFIED BY 65179/DMH/KSR/RW
ON 06-07-2007

1076786

Drafted By: **[LAST, FIRST, MIDDLE: INITIALS]**

(U) **Case ID #:** ~~(S)~~ **[CASE FILE NUMBER]** (Pending)

Title: ~~(S)~~ **[SUBJECT]**
(U) **[AKA [ALIAS] (IF APPLICABLE)**
[FCI/IT - FOREIGN POWER]
[OO: OFFICE OF ORIGIN]

Synopsis: (U) (NSLETR) Approves the issuance of an Electronic Communication Privacy Act (ECPA) National Security Letter (NSL) for electronic communications transactional records; provides reporting data; and, if necessary, transmits the NSL for delivery to the electronic communications service provider.

~~SECRET~~

~~SECRET~~

(U) To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**
Re: (S) **[CASE FILE NUMBER, 00/00/2007]**

(U) (S) ~~**Derived From : G-3**~~
~~**Declassify On: [10-25 years based on information in the EC]**~~

[FULL/PRELIMINARY] Investigation Instituted: (S) **[00/00/2007]**

(U) **Reference:** (S) **[CASE FILE NUMBER SERIAL XXX]**

Enclosure(s): (U) Enclosed for **[DELIVERING DIVISION or OFFICE OF ORIGIN, depending on whether service is personal or through restricted delivery service or fax]** is an NSL dated **[00/00/2006]**, addressed to **[COMPANY POC NAME]**, **[TITLE, (if available)]**, **[COMPANY NAME]**, **[COMPANY ADDRESS - NO P.O. BOX]**, **[CITY, STATE - NO ZIP CODE if using personal service]**, requesting the names, addresses, lengths of service, and electronic transactional records for the **[e-mail/IP]** address holder(s) listed.

(U) **Details:** (S) A **[FULL/PRELIMINARY] [FOREIGN COUNTERINTELLIGENCE/ INTERNATIONAL TERRORISM]** investigation of subject, a **[U.S. PERSON/NON-U.S. PERSON]**, was authorized in accordance with the Attorney General Guidelines because **[Give a full explanation of the justification for opening and maintaining the investigation on the subject. Barebones facts will not suffice and will cause the request to be rejected for legal insufficiency]**. These electronic communications transactional records are being requested to **[Fully state the relevance of the requested records to the investigation]**.

(U) (S) This electronic communication documents the **[APPROVING OFFICIAL's]** approval and certification of the enclosed NSL. For mandatory reporting purposes, the enclosed NSL seeks electronic communication transactional records on **[NUMBER OF] [e-mail/IP address(es)]** from **[ISP #1]; [NUMBER OF] [e-mail/IP address(es)]** from **[ISP #2]**, etc. **[In the case of multiple addresses to the same ISP, if you know how many different persons attach to those addresses, please state. Provide the USP status of all the persons about whom the requests are seeking information, including the subject of the investigation. In other words, do your best to give as much information as you can, for congressional reporting purposes.]**

(U) Arrangements should be made with the electronic communications service provider to provide the records **[personally to an employee of the DELIVERING division** OR **through use of a delivery service or secure fax to OFFICE OF ORIGIN]** within [**NUMBER OF**] business days of receipt of this request. The electronic communications service provider should neither send the records through routine mail service nor utilize the name of the subject of the request in any telephone calls to the FBI.

~~SECRET~~

~~SECRET~~

To: [DELIVERING DIVISION] From: [DRAFTING DIVISION]
(U) Re: ~~(S)~~ [CASE FILE NUMBER, 00/00/2007]

[Certification and Activation of the Nondisclosure Requirement: There is no longer an automatic prohibition that prevents the recipient of a National Security Letter from disclosing that the FBI has requested the information. To activate the nondisclosure requirement, the senior FBI official approving this EC must use Option 1 below and include in the EC (but not in the NSL) a brief statement of facts that justify the nondisclosure requirement. Option 2 is to be used in all cases where Option 1 is not used.]

DISCLOSURE PROVISIONS

[Option 1 - Invoking Nondisclosure Requirement]

(U) In accordance with 18 U.S.C. § 2709(c) I, the senior official approving this EC, certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person.

(S) Brief statement of the facts justifying my certification in this case:

[Option 2 - Declining to invoke the nondisclosure requirement]

(U) I, the senior official approving this EC, have determined that the facts of this case do not warrant activation of the nondisclosure requirements under the applicable National Security Letter statute.

[Include the next 2 paragraphs in all ECs.]

(U) Information received from an electronic communications service provider may be disseminated in accordance with the Attorney General Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(U) Any questions regarding the above can be directed to **[CASE AGENT, telephone number (000) 000-0000]**.

~~SECRET~~

~~SECRET~~

(U) To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**
Re: ~~(S)~~ **[CASE FILE NUMBER, 00/00/2007]**

LEAD(s):

Set Lead 1: (Action)

GENERAL COUNSEL

AT WASHINGTON, DC

(U) NSLB is requested to record the appropriate information needed to fulfill the Congressional reporting requirements for NSLs.

Set Lead 2: (Info)

[COUNERTERRORISM/COUNTERINTELLIGENCE/CYBER]

AT WASHINGTON, DC

(U) At **[Unit]** Read and Clear.

Set Lead 3: (Action)

[DELIVERING DIVISION - if using personal service]

[AT CITY, STATE]

(U) Deliver the attached NSL as indicated above. Upon receipt of information from the electronic communication service provider, **[DELIVERING DIVISION]** is requested to submit results to **[DRAFTING DIVISION]** and **[OFFICE OF ORIGIN, if applicable]**.

♦♦

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ COVER SHEET 05/02/2007

Total Deleted Page(s) ~ 1
Page 4 ~ b2, b7E

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

[DRAFTING DIVISION]
[STREET ADDRESS]
[CITY, STATE, ZIP CODE]
[MONTH, DAY, YEAR]

[MR./MRS./MS.] [COMPLETE NAME OF POC]
[TITLE, IF AVAILABLE]
[NAME OF COMPANY]
[PHYSICAL STREET ADDRESS - NO P.O. BOX]
[CITY, STATE - NO ZIP CODE]

1076786

DEAR **[MR./MRS./MS.] [LAST NAME]:**

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (Section 201 of the Electronic Communications Privacy Act of 1986) (as amended), you are hereby directed to provide to the Federal Bureau of Investigation (FBI) the name, address, length of service, and local and long distance toll billing records associated with the following:

[NAME, IF KNOWN]

[ADDRESS, IF KNOWN]

[TELEPHONE NUMBER(S), IF KNOWN (000) 000-000]:

[RELEVANT TIME PERIOD]: [ON SPECIFIC DATE(S)]

or **[FROM [SPECIFIC DATE] to [[SPECIFIC DATE] or [PRESENT]]**

Please see the attachment following this letter for the types of information that you might consider to be a toll billing record.

If the time period noted above is to the "present," that term is intended to direct production of information to the date of the processing of this letter. If providing information to the date of processing is not feasible, please provide information to the date of receipt of this letter.

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or

clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

[Certification: The nondisclosure requirement is not an automatic feature of the NSL. If the supporting EC for this NSL included Option 1 (Invoking the Nondisclosure Requirement) then include the language in the following 3 paragraphs in the NSL.]

In accordance with 18 U.S.C. § 2709(c)(1), I certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person. Accordingly, 18 U.S.C. § 2709(c)(1) and (2) prohibits you, or any officer, employee, or agent of yours, from disclosing this letter, other than to those to whom disclosure is necessary to comply with the letter or to an attorney to obtain legal advice or legal assistance with respect to this letter.

In accordance with 18 U.S.C. § 2709(c)(3), you are directed to notify any persons to whom you have disclosed this letter that they are also subject to the nondisclosure requirement and are therefore also prohibited from disclosing the letter to anyone else.

In accordance with 18 U.S.C. § 2709(c)(4), if the FBI asks for the information, you should identify any person to whom such disclosure has been made or to whom such disclosure will be made. In no instance will you be required to identify any attorney to whom disclosure was made or will be made in order to obtain legal advice or legal assistance with respect to this letter.

[Include the following language in all NSLs.]

In accordance with 18 U.S.C. § 3511(a) and (b)(1), you have a right to challenge this letter if compliance would be unreasonable, oppressive, or otherwise unlawful, and you have the right to challenge the nondisclosure requirement, if one is set forth above.

In accordance with 18 U.S.C. § 3511(c), an unlawful failure to comply with this letter, including any nondisclosure requirement, may result in the United States bringing an enforcement action.

You are directed to provide records responsive to this letter **[personally to a representative of the [DELIVERING DIVISION]** OR **through use of a delivery service to [OFFICE OF ORIGIN]** OR **through secure facsimile]** within [xxxx] business days of receipt of this letter.

Any questions you have regarding this letter should be directed only to the **[[DELIVERING DIVISION]** OR **[OFFICE OF ORIGIN],_depending on whether service is personal or through a delivery service]**. Due to security considerations, you should neither send the records through routine mail service nor non-secure fax, nor disclose the substance of this letter in any telephone conversation.

Your cooperation in this matter is greatly appreciated.

Sincerely yours,

[ADIC/SAC NAME]
[ASSISTANT DIRECTOR IN CHARGE/
SPECIAL AGENT IN CHARGE]

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: **00/00/2007**

To: General Counsel **Attn:** Julie Thomas
Deputy General Counsel, NSLB

[COUNTERTERRORISM/ COUNTERINTELLIGENCE/CYBER] **Attn: [UNIT]**

[REQUESTING OFFICE] **Attn:** SSA **[SQUAD SUPERVISOR]**
SA **[CASE AGENT]**

[OFFICE OF ORIGIN] **Attn:** SA **[CASE AGENT]**
[Squad] [X]

[DELIVERING DIVISION] **Attn:** SSA **[SQUAD SUPERVISOR]**
(if using personal service) **[Squad] [X]**

From: [**DRAFTING DIVISION**]
[**APPROVING OFFICIAL**]
Contact: [CASE AGENT, telephone number (000) 000-0000]

Approved By: **[ADIC NAME (IF APPLICABLE]**
[SAC NAME]
[ASAC NAME]
[CDC NAME]
[SSA NAME]

DECLASSIFIED BY 65179/DMH/KSR/RW
ON 06-07-2007
1076786

Drafted By: **[LAST, FIRST, MIDDLE NAME: INITIALS]**

(U) **Case ID #:** ~~(S)~~ **[CASE FILE NUMBER]** (Pending)

(U) **Title:** ~~(S)~~ **[SUBJECT]**
[AKA] [ALIAS IF APPLICABLE]
[IT/FCI - FOREIGN POWER];
[OO: OFFICE OF ORIGIN]

Synopsis: (U) (NSLTTR) Approves the issuance of an Electronic Communication Privacy Act (ECPA) National Security Letter (NSL) for toll billing records; provides reporting data; and, if

~~SECRET~~

To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**
(U) Re: ~~(S)~~ **[CASE FILE NUMBER, 00/00/2007]**

necessary, transmits the NSL for delivery to the wire communications service provider.

(U) ~~(S)~~ ~~**Derived From: G-3**~~
~~**Declassify On: [10-25 years based on information in the EC]**~~

(U) **[FULL/PRELIMINARY] Investigation Instituted:** ~~(S)~~ **[00/00/2007]**

(U) **Reference:** ~~(S)~~ **[CASE FILE NUMBER Serial XXX]**

Enclosures: (U) Enclosed for **[DELIVERING DIVISION or OFFICE OF ORIGIN, depending on whether service is personal or through restricted delivery service or fax]** is an NSL dated **[00/00/2006]**, addressed to **[COMPANY POC NAME]**, **[TITLE (if available)]**, **[COMPANY NAME]**, **[COMPANY ADDRESS - NO P.O. BOX]**, [**CITY, STATE - NO ZIP CODE if using personal service]**, requesting the name, address, length of service and local and long distance toll billing records for the phone number(s) listed.

(U) **Details:** ~~(S)~~ A **[FULL/PRELIMINARY] [INTERNATIONAL TERRORISM/FOREIGN COUNTERINTELLIGENCE]** investigation of subject, a **[USPER/NON-USPER]**, was authorized in accordance with the Attorney General Guidelines because **[Give a full explanation of the justification for opening and maintaining the investigation on the subject; barebones facts will not suffice and will cause the request to be rejected for legal insufficiency]**. These toll billing records are being requested to **[Fully state the relevance of the requested records to the investigation]**.

(U) ~~(S)~~ This electronic communication documents the **[APPROVING OFFICIAL's]** approval and certification of the enclosed NSL. For mandatory reporting purposes, the enclosed NSL seeks local and long distance toll billing records for **[NUMBER OF]** telephone number(s) from **[telephone company #1]**; **[NUMBER OF]** telephone number(s) from **[telephone company #2]**, etc. **[In the case of multiple phone numbers to the same telephone company, if you know how many different persons attach to those phone numbers, please state. Provide the USP status of all the persons about whom the requests are seeking information, including the subject of the investigation. In other words, do your best to**

(U) To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**
Re: ~~(S)~~ **[CASE FILE NUMBER, 00/00/2007]**

give as much information as you can, for congressional reporting purposes.]

(U) Arrangements should be made with the wire communications service provider to provide the records **[personally to an employee of the DELIVERING DIVISION** OR **through use of a delivery service or secure fax to OFFICE OF ORIGIN]** within [**NUMBER OF**] business days of receipt of this request. The wire communications service provider should neither send the records through routine mail service nor utilize the name of the subject of the request in any telephone calls to the FBI.

DISCLOSURE PROVISIONS

[Certification and Activation of the Nondisclosure Requirement: There is no longer an automatic prohibition that prevents the recipient of a National Security Letter from disclosing that the FBI has requested the information. To activate the nondisclosure requirement, the senior FBI official approving this EC must use Option 1 below and include in the EC (but not in the NSL) a brief statement of facts that justify the nondisclosure requirement. Option 2 is to be used in all cases where Option 1 is not used.]

[Option 1 - Invoking Nondisclosure Requirement]

(U) In accordance with 18 U.S.C. § 2709(c) I, the senior official approving this EC, certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person.

(U) ~~(S)~~ Brief statement of the facts justifying my certification in this case:

[Option 2 - Declining to invoke the nondisclosure requirement]

(U) I, the senior official approving this EC, have determined that the facts of this case do not warrant activation of the nondisclosure requirements under the applicable National Security Letter statute.

(U) To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**
Re: ~~(S)~~ **[CASE FILE NUMBER, 00/00/2007]**

[Include the next 2 paragraphs in all ECs.]

(U) Information received from a wire communication service provider may be disseminated in accordance with the Attorney General Guidelines on National Security Investigations and Foreign Intelligence Collection and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(U) Any questions regarding the above can be directed to **[CASE AGENT, telephone number (000) 000-0000]**.

~~SECRET~~

(U) To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**
Re: ~~(S)~~ **[CASE FILE NUMBER, 00/00/2007]**

LEAD ~~(s)~~:

Set Lead 1:

GENERAL COUNSEL

AT WASHINGTON, DC

(U) NSLB is requested to record the appropriate information needed to fulfill the Congressional reporting requirements for NSLs.

Set Lead 2: (Info)

[COUNTERTERRORISM/COUNTERINTELLIGENCE/CYBER]

AT WASHINGTON, DC

(U) At **[Unit]** Read and Clear

Set Lead 3:

[DELIVERING DIVISION - if using personal service]

[AT [CITY, STATE]

(U) Deliver the attached NSL as indicated above. Upon receipt of information from the wire communications service provider, **[DELIVERING DIVISION]** is requested to submit results to the **[DRAFTING DIVISION]** and **[OFFICE OF ORIGIN, if applicable]**.

♦♦

~~SECRET~~

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

[DRAFTING DIVISION]
[STREET ADDRESS]
[CITY, STATE, ZIP CODE]

[MONTH, DAY, YEAR]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-07-2007 BY 65179/DMH/KSR/RW

[MR./MRS./MS.] [Complete name]
[TITLE, IF AVAILABLE]
[NAME OF COMPANY]
[PHYSICAL STREET ADDRESS - NO P.O. BOX]
[CITY, STATE - NO ZIP CODE]

1076786

Dear **[MR./MRS./MS.] [LAST NAME]:**

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (Section 201 of the Electronic Communications Privacy Act of 1986) (as amended), you are hereby directed to provide to the Federal Bureau of Investigation (FBI) the name, address, and length of service with respect to the following telephone number(s):

[provide either or both - 1) person(s) to whom the telephone number(s) is/was registered and/or 2) the telephone number(s)]

[NAME OF PERSON(S)]

[TELEPHONE NUMBER(S) (000) 000-000)]:

[RELEVANT TIME PERIOD]: [ON SPECIFIC DATE]

or **[FROM [SPECIFIC DATE] to [SPECIFIC DATE] or [PRESENT]]**

If the time period noted above is to the "present," that term is intended to direct production of information to the date of the processing of this letter. If providing information to the date of processing is not feasible, please provide information to the date of receipt of this letter.

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an

investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the constitution of the United States.

[Certification: The nondisclosure requirement is not an automatic feature of the NSL. If the supporting EC for this NSL included Option 1 (Invoking the Nondisclosure Requirement) then include the language in the following 3 paragraphs in the NSL.]

In accordance with 18 U.S.C. § 2709(c)(1), I certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person. Accordingly, 18 U.S.C. § 2709(c)(1) and (2) prohibits you, or any officer, employee, or agent of yours, from disclosing this letter, other than to those to whom disclosure is necessary to comply with the letter or to an attorney to obtain legal advice or legal assistance with respect to this letter.

In accordance with 18 U.S.C. § 2709(c)(3), you are directed to notify any persons to whom you have disclosed this letter that they are also subject to the nondisclosure requirement and are therefore also prohibited from disclosing the letter to anyone else.

In accordance with 18 U.S.C. § 2709(c)(4), if the FBI asks for the information, you should identify any person to whom such disclosure has been made or to whom such disclosure will be made. In no instance will you be required to identify any attorney to whom disclosure was made or will be made in order to obtain legal advice or legal assistance with respect to this letter.

[Include the following language in all NSLs.]

In accordance with 18 U.S.C. § 3511(a) and (b)(1), you have a right to challenge this letter if compliance would be unreasonable, oppressive, or otherwise unlawful, and you have the right to challenge the nondisclosure requirement set forth above.

In accordance with 18 U.S.C. § 3511(c), an unlawful failure to comply with this letter, including any nondisclosure requirement, may result in the United States bringing an enforcement action.

[MR./MRS./MS] [COMPLETE NAMES]

You are directed to provide records responsive to this letter **[personally to a representative of the [DELIVERING DIVISION]** OR **through use of a delivery service to [OFFICE OF ORIGIN]** OR **through secure fax]** within [xxxx] business days of receipt of this letter.

Any questions you have regarding this letter should be directed only to the **[[DELIVERING DIVISION]** OR **[OFFICE OF ORIGIN],_depending on whether service is personal or through a delivery service]**. Due to security considerations, you should neither send the records through routine mail service nor non-secure fax, nor disclose the substance of this letter in any telephone conversation.

Your cooperation in this matter is greatly appreciated.

Sincerely yours,

[ADIC/SAC NAME]
[ASSISTANT DIRECTOR IN CHARGE/
SPECIAL AGENT IN CHARGE]

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: **00/00/2007**

To: General Counsel **Attn:** Julie Thomas
Deputy General Counsel, NSLB

[COUNTERTERRORISM/ COUNTERINTELLIGENCE/CYBER] **Attn: [UNIT]**

[REQUESTING OFFICE] **Attn:** SSA **[SQUAD SUPERVISOR]**
SA **[CASE AGENT]**

[OFFICE OF ORIGIN] **Attn:** SA **[CASE AGENT]**
[Squad] [X]

[DELIVERING DIVISION] **Attn:** SSA **[SQUAD SUPERVISOR]**
(if using personal service) **[Squad] [X]**

From: [**DRAFTING DIVISION**]
[**APPROVING OFFICIAL**]
Contact: [CASE AGENT, telephone number (000) 000-0000]

Approved By: **[ADIC NAME (IF APPLICABLE]**
[SAC NAME]
[ASAC NAME]
[CDC NAME]
[SSA NAME]

DECLASSIFIED BY 65179/DMH/KSR/RW
ON 06-07-2007

1076786

Drafted By: **[LAST, FIRST, MIDDLE NAME: INITIALS]**

(U) **Case ID #:** ~~(S)~~ **[CASE FILE NUMBER]** (Pending)

(U) **Title:** ~~(S)~~ **[SUBJECT]**
[AKA] [ALIAS IF APPLICABLE]
[IT/FCI - FOREIGN POWER];
[OO: OFFICE OF ORIGIN]

Synopsis: (U) (NSLTTR) Approves the issuance of an Electronic Communication Privacy Act (ECPA) National Security Letter (NSL) for toll billing records; provides reporting data; and, if

~~SECRET~~

(U) To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**
Re: (S) **[CASE FILE NUMBER, 00/00/2007]**

necessary, transmits the NSL for delivery to the wire communications service provider.

(U) (S) ~~**Derived From: G-3**~~
~~**Declassify On: [10-25 years based on information in the EC]**~~

(U) **[FULL/PRELIMINARY] Investigation Instituted:** (S) **[00/00/2007]**

(U) **Reference:** (S) **[CASE FILE NUMBER Serial XXX]**

Enclosures: (U) Enclosed for **[DELIVERING DIVISION or OFFICE OF ORIGIN, depending on whether service is personal or through restricted delivery service or fax]** is an NSL dated **[00/00/2006]**, addressed to **[COMPANY POC NAME]**, **[TITLE (if available)]**, **[COMPANY NAME]**, **[COMPANY ADDRESS - NO P.O. BOX]**, [**CITY, STATE - NO ZIP CODE if using personal service]**, requesting the name, address, length of service and local and long distance toll billing records for the phone number(s) listed.

(U) **Details:** (S) A **[FULL/PRELIMINARY] [INTERNATIONAL TERRORISM/FOREIGN COUNTERINTELLIGENCE]** investigation of subject, a **[USPER/NON-USPER]**, was authorized in accordance with the Attorney General Guidelines because **[Give a full explanation of the justification for opening and maintaining the investigation on the subject; barebones facts will not suffice and will cause the request to be rejected for legal insufficiency]**. These toll billing records are being requested to **[Fully state the relevance of the requested records to the investigation]**.

(U) (S) This electronic communication documents the **[APPROVING OFFICIAL's]** approval and certification of the enclosed NSL. For mandatory reporting purposes, the enclosed NSL seeks local and long distance toll billing records for **[NUMBER OF]** telephone number(s) from **[telephone company #1]**; **[NUMBER OF]** telephone number(s) from **[telephone company #2]**, etc. **[In the case of multiple phone numbers to the same telephone company, if you know how many different persons attach to those phone numbers, please state. Provide the USP status of all the persons about whom the requests are seeking information, including the subject of the investigation. In other words, do your best to**

~~SECRET~~

(U) To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**
Re: ~~(S)~~ **[CASE FILE NUMBER, 00/00/2007]**

give as much information as you can, for congressional reporting purposes.]

(U) Arrangements should be made with the wire communications service provider to provide the records **[personally to an employee of the DELIVERING DIVISION** OR **through use of a delivery service or secure fax to OFFICE OF ORIGIN]** within [**NUMBER OF**] business days of receipt of this request. The wire communications service provider should neither send the records through routine mail service nor utilize the name of the subject of the request in any telephone calls to the FBI.

DISCLOSURE PROVISIONS

[Certification and Activation of the Nondisclosure Requirement: There is no longer an automatic prohibition that prevents the recipient of a National Security Letter from disclosing that the FBI has requested the information. To activate the nondisclosure requirement, the senior FBI official approving this EC must use Option 1 below and include in the EC (but not in the NSL) a brief statement of facts that justify the nondisclosure requirement. Option 2 is to be used in all cases where Option 1 is not used.]

[Option 1 - Invoking Nondisclosure Requirement]

(U) In accordance with 18 U.S.C. § 2709(c) I, the senior official approving this EC, certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person.

(U) ~~(S)~~ Brief statement of the facts justifying my certification in this case:

[Option 2 - Declining to invoke the nondisclosure requirement]

(U) I, the senior official approving this EC, have determined that the facts of this case do not warrant activation of the nondisclosure requirements under the applicable National Security Letter statute.

~~SECRET~~

(U) To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**
Re: ~~(S)~~ **[CASE FILE NUMBER, 00/00/2007]**

[Include the next 2 paragraphs in all ECs.]

(U) Information received from a wire communication service provider may be disseminated in accordance with the Attorney General Guidelines on National Security Investigations and Foreign Intelligence Collection and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(U) Any questions regarding the above can be directed to **[CASE AGENT, telephone number (000) 000-0000]**.

~~SECRET~~

To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**
(U) Re: ~~(S)~~ **[CASE FILE NUMBER, 00/00/2007]**

LEAD (s):

Set Lead 1:

GENERAL COUNSEL

AT WASHINGTON, DC

(U) NSLB is requested to record the appropriate information needed to fulfill the Congressional reporting requirements for NSLs.

Set Lead 2: (Info)

[COUNTERTERRORISM/COUNTERINTELLIGENCE/CYBER]

AT WASHINGTON, DC

(U) At **[Unit]** Read and Clear

Set Lead 3:

[DELIVERING DIVISION - if using personal service]

[AT [CITY, STATE]

(U) Deliver the attached NSL as indicated above. Upon receipt of information from the wire communications service provider, **[DELIVERING DIVISION]** is requested to submit results to the **[DRAFTING DIVISION]** and **[OFFICE OF ORIGIN, if applicable]**.

♦♦

~~SECRET~~

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 04/11/2006

To: Counterterrorism **Attn:** AD, DAD

Counterintelligence AD, DAD

Cyber Acting AD, DAD

All Field Offices ADIC
SAC
CDC

From: Office of the General Counsel
National Security Law Branch LX-1 Room 3S100
Contact: [redacted]

Approved By: Caproni Valerie E
Hulon Willie T
Bereznay Timothy P

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-07-2007 BY 65179/DMH/KSR/RW

1076786

b6
b7C
b2

Drafted By: [redacted]

Case ID #: 319X-HQ-A1487720-OGC

Title: LEGAL ADVICE AND OPINIONS;
FBI POLICY RE REIMBURSEMENT OF COSTS TO RECIPIENTS
OF NATIONAL SECURITY LETTERS

Synopsis: Provides guidance to the field as to the establishment within the FBI of a uniform policy with respect to reimbursement of costs to recipients of National Security Letters (NSLs) for the production of information responsive to NSLs. This guidance provides that where the authorizing statute requires reimbursement, clearly we will continue our practice of paying. Where the authorizing statute does not reference any form of reimbursement, then the FBI will not pay for the information.

Details:

Four statutes that provide for the issuance of National Security Letters vary in their provision for reimbursement of costs to recipients of NSLs for production of information responsive to NSLs. The Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709, does not provide for reimbursement of costs; thus, there is no legal obligation to pay for toll billing/subscriber records or electronic communication transactional records to which the statute applies. The Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3415, requires

reimbursement of costs for information obtained from financial institutions to which NSLs are issued under Section 3414(a)(5)(A); Title 12, Code of Federal Regulations (CFR), Part 219, and Appendix A, provides a reimbursement of costs schedule.[1] The Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681u, requires reimbursement of costs for financial institution listings and consumer identifying information obtained from credit reporting companies but no reimbursement schedule has been promulgated.[2] Its counterpart, FCRA, Section 1681v, enacted as part of the 2001 USA Patriot Act, providing for full credit reports in international terrorism cases, does not authorize reimbursement of costs.

Variations in Cost Reimbursement Policy Among FBI Field Offices

The differences in the payment provisions of the NSL statutes have caused field offices to adopt varying policies as to whether they pay bills that are submitted by NSLs recipients. When bills are submitted by RFPA NSL recipients, the rules are clear. Field offices must and do pay for such NSLs based on the reimbursement of costs schedule set out in the CFR. When bills are submitted by ECPA NSL recipients, where reimbursement is not required, some field offices pay the bills as submitted, others negotiate the amount of the charge, and others flatly refuse to pay. As to credit reporting companies responding to 1681v NSLs,[3] at least one such company submits bills which, to date, we have paid. With respect to credit reporting companies responding to 1681u NSLs, at least two have a policy of submitting bills, which we pay or intend to pay. While there is no fee schedule

---

[1] RFPA, Section 3415 provides that "a Government entity shall pay to the financial institution assembling or providing financial records pertaining to a customer and in accordance with procedures established by this chapter a fee for reimbursement of costs as reasonably necessary and which have been directly incurred in searching for, reproducing, or transporting books, papers, records, or other data required ro requested to be produced. The Board of Governors of the Federal Reserve System shall, by regulation, establish the rates and conditions under which such payment shall be made. Under 12 C.F.R. §219.3, Appendix A, a fee schedule has been adopted, under which photocopying is reimbursable at $.25 per page and searching is reimbursable at $11 per hour for clerical staff.

[2] FCRA, Section 1681u(e) provides that "[t]he Federal Bureau of Investigation shall, subject to the availability of appropriations, pay to the consumer reporting agency assembling or providing report or information in accordance with procedures established under this section a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching, reproducing, or transporting books, papers, records, or other data required or requested to be produced under this section."

[3] The three major credit reporting companies are Experien, Transunion, and Equifax.

established, the fees that are or will be charged by credit reporting companies for 1681u requests are approximately ten dollars, which appears reasonable, as well as in line with the hourly rate set by the RFPA schedule.[4]

The Problem to be Addressed by this Guidance

Having canvassed FBI field offices as to whether they would like to see the FBI adopt a uniform policy with respect to reimbursement of costs of NSL recipients, the Office of the General Counsel (OGC) has determined that field offices do in fact want a uniform policy. That is the genesis of this guidance. However, since this is an operational issue and not a legal issue, OGC has also obtained the concurrence of the FBI's Counterterrorism Division, Counterintelligence Division, and Cyber Division that a uniform policy is desirable. Thus, this guidance is intended to create a uniform policy as to reimbursement of costs of NSL recipients, the creation of which uniform policy is particularly crucial with respect to those statutes which do not provide for compensation, such as ECPA and FCRA Section 1681v.

Reimbursement of Costs Incurred by ECPA NSL recipients

The FBI hereby adopts the policy that, since it has no legal obligation to reimburse costs incurred by an NSL recipient in producing information sought by an ECPA NSL, that it will not pay bills that are submitted by ECPA NSL recipients for such information. Its position is supported by the fact that the ECPA specifically provides for certain instances in which compensation to recipients of legal process is available. Those enumerated provisions do not include Section 2709.[5] Further, since certain NSL statutes do contain reimbursement provisions, it is clear that when Congress so intended, it did in fact enact such a provision. While there is not necessarily any obvious rationale to the determination of which NSL statutes contain reimbursement provisions, the fact is that Congress has had opportunities to remedy what may have been an oversight in the ECPA provision and has not done so. [redacted] b5

[4] Transunion currently charges ten dollars for 1681u requests, but does not charge for 1681v requests. Experien currently charges $9.20 per report.

[5] Title 18, Section 2706(a) of ECPA provides for a reimbursement fee for obtaining "the contents of communications, records, or other information under section 2702, 2703, or 2704," except the provision does not apply, per section 2706(c), "with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider."

b5

[redacted]

Further, to the extent that bills for reimbursement submitted by carriers in the past have been paid by field offices, they presumably have been done so on the theory that payment will encourage cooperation and responsiveness to an NSL request. Inasmuch as the NSL statutes were revised by the USA PATRIOT Act Improvement and Reauthorization Act of 2005 to provide for an enforcement mechanism, there is less of a need for the FBI to seek voluntary cooperation of carriers by providing payment to which the carriers are not legally entitled.

Enclosed is a model letter that field offices may want to use in response to requests for payment. These letters may assume particular importance when addressed to carriers who to date have received reimbursement and suddenly find themselves cut off from reimbursement under the new FBI policy.

Reimbursement of Costs Incurred by FCRA Section 1681v NSL Recipients

[redacted]

b5

At the current time, Transunion does not charge for 1681v NSL requests.

Reimbursement of Costs Incurred by FCRA Section 1681u NSL Recipients

While FCRA Section 1681u provides for compensation for NSLs, there has yet to be promulgated a schedule of such fees. Inasmuch as a separate fee schedule has not been adopted, it is logical that the fee schedule adopted for RFPA NSLs be the basis of compensation for Section 1681u NSLs. [redacted]

b2
b7E

[redacted], there should also be flexibility in how [redacted] offices handle such bills. We recommend that they coordinate with one another

so that the compensation is uniform, as well as generally in line with the RFPA fee schedule. [redacted]

b5
b2
b7E

[redacted]

Conclusion

OGC recognizes that field offices are likely to need further guidance when faced with particular scenarios. There may be situations in which lack of compensation is unduly harsh in light of the burden placed on the carrier by an NSL request. Such situations may be addressed on a case-by-case basis.[6]

To the extent that there are repercussions with respect to the compliance with NSLs, we do now have in place an enforcement mechanism for NSLs via the recently enacted USA PATRIOT Act Improvement and Reauthorization Act of 2005. That statutory authority should serve to ameliorate the possible adverse consequences that might ensue at the onset of this new policy.

Any questions about the issues set forth above should be addressed to field office Chief Division Counsel or to [redacted] in the National Security Law Branch ((571)280-[redacted]

b6
b7C
b2

[redacted]

LEAD(s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Distribute to all supervisory personnel involved in the investigation of counterintelligence, counterterrorism, and cyber cases.

1 - Ms. Caproni
1 - Mr. Hulon
1 - Mr. Bereznay
1 - [redacted]
1 - [redacted]
♦♦

b6
b7C

---

[6] This flexibility is conceptually analogous to the provision of ECPA, Section 2706, which authorizes court-ordered compensation when a criminal legal process seeking telephone records is especially burdensome. See footnote 5.

SUGGESTED FORM LETTER TO NSL RECIPIENT

[Name and address of NSL recipient]

1073946

RE: Cost Reimbursement for National Security Letter
Invoice No: ___ (if relevant)
Invoice Dated: ___ (if relevant)

Dear (POC),

This letter references the above invoice directed to this office in which you request payment for producing records to the FBI in response to a National Security Letter (NSL) issued on [Date of Issuance].

The federal statute under which the NSL to your company was issued, [**Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709, or Fair Credit Reporting Act, 15 U.S.C. § 1681v**], does not authorize cost reimbursement. [**FOR ECPA:** While certain other methods of legal process are subject to cost reimbursement under ECPA, Section 2706, the enumerated list of provisions does not include Section 2709.] [**For FCRA:** While certain other methods of legal process are subject to cost reimbursement under FCRA, including Section 1681u, there is no such comparable provision for cost reimbursement for Section 1681v.] Therefore, absent a specific provision providing for cost reimbursement, no entity or person is entitled to reimbursement for complying with federal legal process. Hurtado v. United States, 410 U.S. 578 (1973).

Therefore, it is the FBI's position that cost reimbursement for NSL compliance is not specifically authorized under [**ECPA Section 2709 or FCRA Section 1681v**].

[**TO BE USED FOR RECIPIENTS WHO HAVE BEEN REIMBURSED IN THE PAST:** We recognize that in the past, your company may have been reimbursed for compliance with NSLs. However, the FBI has reevaluated its position in that regard and determined that in order to assure fair and equal treatment of all NSL recipients, a uniform posture is required as to the appropriateness of reimbursing recipients of NSLs for their compliance in the absence of statutory authorization for such reimbursement. The FBI has decided that payment is not appropriate in these circumstances.]

Please feel free to contact the undersigned should you wish to discuss this further. This office greatly appreciates your timely compliance with NSL requests, which assists us in fulfilling our investigative responsibilities and efforts to further the national security interests of this country.

Sincerely yours,

[NAME OF SAC or SSA]
[Position]
[Name of Field Office]

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ COVER SHEET 05/02/2007

Total Deleted Page(s) ~ 2
Page 5 ~ b2, b7E
Page 6 ~ b2, b7E

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

[DRAFTING DIVISION]
[STREET ADDRESS]
[CITY,STATE, ZOP CODE]
[MONTH DAY, YEAR]

[MR./MRS/MS.] [COMPLETE POC NAME]
[TITLE, IF AVAILABLE]
[COMPANY NAME]
[PHYSICAL STREET ADDRESS - NO P.O. BOX]
[CITY, STATE - NO ZIP CODE]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-07-2007 BY 65179/DMH/KSR/RW

1076786

DEAR [MR./MRS./MS.] [LAST NAME]:

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 12, United States Code (U.S.C.), Section 3414(a)(5), you are hereby directed to produce to the Federal Bureau of Investigation (FBI) all financial records pertaining to the customer(s) and/or accounts listed below:

NAME(S) [if available]

ACCOUNT NUMBER(s): [if available]

SOCIAL SECURITY NUMBER(S): [if available]

DATE(S) OF BIRTH: [if available]

[FOR PERIOD FROM INCEPTION TO PRESENT]

or

[FOR PERIOD FROM [SPECIFIC DATE] TO [SPECIFIC DATE]

or [PRESENT]]

Please see the attachment following this letter for the types of information that your financial institution might consider to be a financial record.

If the time period noted above is to the "present," that term is intended to direct production of information to the date of the processing of this letter. If providing information to the date of processing is not feasible, please provide information to the date of receipt of this letter.

[MR./MRS./MS./ COMPLETE NAME]

In accordance with Title 12, U.S.C. Section 3414(a)(5)(A), I certify that these records are sought for foreign counterintelligence investigation purposes to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

In accordance with Title 12, U.S.C., Section 3403(b), I certify that the FBI has complied with all applicable provisions of the Right to Financial Privacy Act.

[Certification: The nondisclosure requirement is not an automatic feature of the NSL. If the supporting EC for this NSL included Option 1 (Invoking the Nondisclosure Requirement) then include the language in the following 3 paragraphs in the NSL.]

In accordance with 12 U.S.C. § 3414(a)(5)(D), I certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person. Accordingly, 12 U.S.C. § 3414(a)(5)(D) prohibits you, or any officer, employee, or agent of yours, from disclosing this letter, other than to those to whom disclosure is necessary to comply with the letter or to an attorney to obtain legal advice or legal assistance with respect to this letter.

In accordance with 12 U.S.C. § 3414(a)(5)(D)(iii), you are directed to notify any persons to whom you have disclosed this letter that they are also subject to the nondisclosure requirement and are therefore also prohibited from disclosing the letter to anyone else.

In accordance with 12 U.S.C. § 3414(a)(5)(D)(iv), if the FBI asks for the information, you should identify any person to whom such disclosure has been made or to whom such disclosure will be made. In no instance will you be required to identify any attorney to whom disclosure was made or will be made in order to obtain legal advice or legal assistance with respect to this letter.

[Include the following language in all NSLs.]

[MR./MRS./MS./ COMPLETE NAME]

In accordance with 18 U.S.C. § 3511(a) and (b)(1), you have a right to challenge this letter if compliance would be unreasonable, oppressive, or otherwise unlawful and the right to challenge the nondisclosure requirement set forth above.

In accordance with 18 U.S.C. § 3511(c), an unlawful failure to comply with this letter, including any nondisclosure requirement, may result in the United States bringing an enforcement action.

The FBI does not intend to suggest, by the service of the NSL upon your financial institution [redacted] the non-disclosure provision set forth above prohibits the disclosure of the fact of this letter [redacted] Further, should you decide to consider [redacted] the FBI requests that you please notify the below point of contact prior to taking such action, inasmuch as it is expected that information [redacted]

b2
b7E

You are directed to provide records responsive to this letter **[personally to a representative of the [DELIVERING DIVISION]** OR **through use of a delivery service to the [OFFICE OF ORIGIN]** OR **through secure fax]** within [xxxx] business days of receipt of this letter.

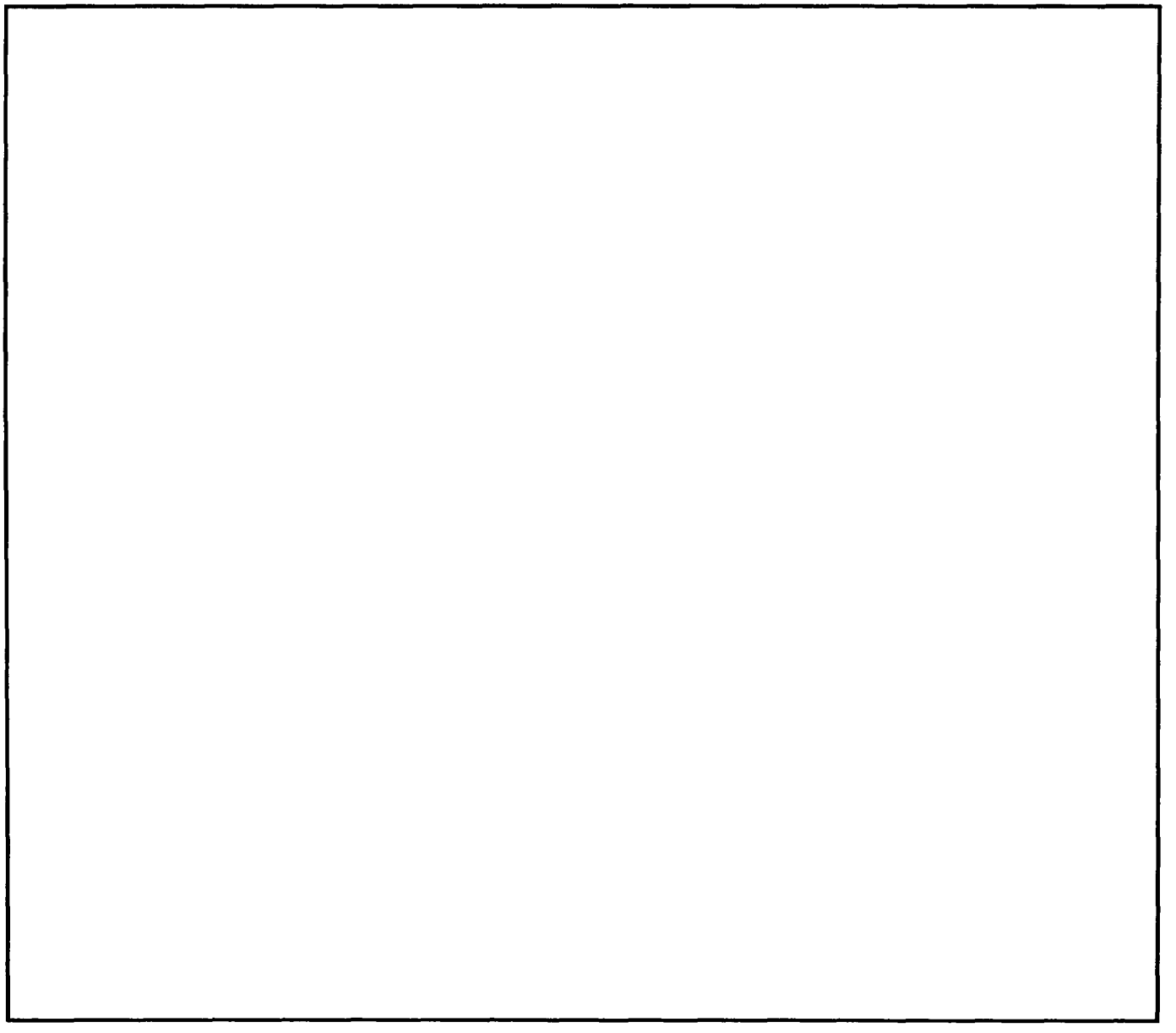
Any questions you have regarding this letter should be directed only to the **[[DELIVERING DIVISION]** OR **[OFFICE OF ORIGIN],_depending on whether service is personal or through a delivery service or fax]**. Due to security considerations, you should neither send the records through routine mail service nor disclose the substance of this letter in any telephone conversation.

Your cooperation in this matter is greatly appreciated.

Sincerely,

[ADIC/SAC NAME]
[ASSISTANT DIRECTOR IN CHARGE/
SPECIAL AGENT IN CHARGE]

b2
b7E



(Rev. 01-31-2003)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date: 00/00/2007**

To: General Counsel **Attn:** Julie Thomas
Deputy General Counsel, NSLB

[COUNTERTERRORISM/ COUNTERINTELLIGENCE/CYBER] **Attn: [UNIT]**

[REQUESTING OFFICE] **Attn:** SSA **[SQUAD SUPERVISOR]**
SA **[CASE AGENT]**

[OFFICE OF ORIGIN] **Attn:** SA [**CASE AGENT**]
[**SQUAD**] [**X**]

[DELIVERING DIVISION] **Attn:** SSA [**SQUAD SUPERVISOR**]
(if using personal service) [**SQUAD**] [**X**]

From: [DRAFTING DIVISION]
[APPROVING OFFICIAL]
Contact: [CASE AGENT, telephone number (000) 000-0000]

Approved By: **[ADIC NAME, IF APPLICABLE]**
[SAC NAME]
[ASAC NAME]
[CDC NAME]
[SSA NAME]

Drafted By: **[LAST, FIRST MIDDLE: INITIALS]**

(U) **Case ID #:** ~~(S)~~ **[CASE FILE NUMBER]** (Pending)

DECLASSIFIED BY 65179/DMH/KSR/RW
ON 06-07-2007

(U) **Title:** ~~(S)~~ **[SUBJECT]**
[AKA] [ALIAS, IF APPLICABLE]
[IT/FCI - FOREIGN POWER]
[OO: OFFICE OF ORIGIN]

1076786

Synopsis: (U) (NSLFR) Approves the issuance of an Right to Financial Privacy Act (RFPA) National Security Letter (NSL) for financial records; provides reporting data; and, if necessary, transmits the NSL for delivery to the financial institution.

(U) ~~(S)~~

~~**Derived From : G-3**~~
~~**Declassify On: [10-25 years based on information in the EC]**~~

~~SECRET~~

(U) To: **[CTD/CD]** From: **[DRAFTING DIVISION]**
Re: ~~(S)~~ **[CASE FILE NUMBER, 00/00/2007]**

(U) **[FULL/PRELIMINARY] Investigation Instituted:** ~~(S)~~ **00/00/2007**

(U) **Reference:** ~~(S)~~ **[CASE FILE NUMBER SERIAL XXX]**

Enclosure(s): (U) Enclosed for **[DELIVERING DIVISION or OFFICE OF ORIGIN, depending on whether service is personal or through restricted delivery service]** is an NSL dated **[00/00/2006]**, addressed to **[COMPANY POC NAME], [TITLE (if available)], [COMPANY NAME], [COMPANY ADDRESS - NO P.O. BOX], [CITY, STATE - NO ZIP CODE if using personal service]**, requesting financial records of the customer listed.

(U) **Details:** ~~(S)~~ A **[FULL/PRELIMINARY] [FOREIGN COUNTERINTELLIGENCE/ INTERNATIONAL TERRORISM]** investigation of subject, a **[U.S. PERSON/NON-U.S. PERSON]**, was authorized in accordance with the Attorney General Guidelines because **[Give a full explanation of the justification for opening and maintaining the investigation on the subject; barebones facts will not suffice and will cause the request to be rejected for legal insufficiency]**. These financial records are being requested to **[Fully state the relevance of the requested records to the investigation]**.

(U) ~~(S)~~ This electronic communication documents the **[APPROVING OFFICIAL's]** approval and certification of the enclosed NSL. For mandatory reporting purposes, the enclosed NSL seeks financial records for **[NUMBER OF] [individual(s)/account(s)]** from **[financial institution #1]; [NUMBER OF] [individual(s)/accounts]** from **[financial institution #2]**, etc. **[In the case of multiple accounts to the same financial institution, if you know how many different persons attach to those accounts, please state. Provide the USP status of all the persons about whom the requests are seeking information, including the subject of the investigation. In other words, do your best to give as much information as you can, for congressional reporting purposes.]**

(U) Arrangements should be made with the financial institution to provide the records **[personally to an employee of the DELIVERING DIVISION** OR **through use of a delivery service or secure fax to OFFICE OF ORIGIN]** within **[NUMBER OF]** business days of receipt of this request. The financial institution should neither send the records through routine mail service nor utilize the name of the subject of the request in any telephone calls to the FBI.

DISCLOSURE PROVISIONS

[Option 1 - Invoking Nondisclosure Requirement]

~~SECRET~~

To: **[CTD/CD]** From: **[DRAFTING DIVISION]**
(U) Re: ~~(S)~~ **[CASE FILE NUMBER, 00/00/2007]**

(U) In accordance with 12 U.S.C. § 3414(a)(5)(D), I, the senior official approving this EC, certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person.

(U) ~~(S)~~ Brief statement of the facts justifying my certification in this case:

[Option 2 - Declining to invoke the nondisclosure requirement]

(U) I, the senior official approving this EC, have determined that the facts of this case do not warrant activation of the nondisclosure requirements under the applicable National Security Letter statute.

[Include the next 2 paragraphs in all ECs.]

(U) Information received from a financial institution may be disseminated in accordance with the Attorney General Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(U) Any questions regarding the above can be directed to **[CASE AGENT, telephone number (000) 000-0000]**.

~~SECRET~~

(U) To: [CTD/CD] From: [DRAFTING DIVISION]
Re: ~~(S)~~ [CASE FILE NUMBER, 00/00/2007]

LEAD(s):

Set Lead 1: (Action)

GENERAL COUNSEL

AT WASHINGTON, DC

(U) NSLB is requested to record the appropriate information needed to fulfill the Congressional reporting requirements for NSLs.

Set Lead 2: (Info)

[COUNTERTERRORISM/COUNTERINTELLIGENCE/CYBER]

AT WASHINGTON, DC

(U) At **[Unit]** Read and Clear

Set Lead 3: (Action)

[DELIVERING DIVISION - if using personal service]

[AT CITY, STATE]

(U) Deliver the attached NSL as indicated above. Upon receipt of information from the financial institution, **[DELIVERING DIVISION]** is requested to submit results to **[DRAFTING DIVISION]** and **[OFFICE OF ORIGIN, if applicable]**.

♦♦

~~SECRET~~

(Rev. 03-08-2006)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/9/2006

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

From: Office of the General Counsel National Security Law Branch
Contact: [redacted]

b6
b7C
b2

Approved By: Mueller Robert S III

Drafted By: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-07-2007 BY 65179/DMH/KSR/RW

1076786

Case ID #: 319X-HQ-A1487720-OGC Serial 210

Title: NATIONAL SECURITY LETTERS
DELEGATION OF SIGNATURE AUTHORITY
DELEGATION OF NON-DISCLOSURE CERTIFICATION AUTHORITY
DELEGATION OF NON-DISCLOSURE RECERTIFICATION AUTHORITY

Synopsis: Delegates signature authority for National Security Letters under the Electronic Communications Privacy Act, 18 U.S.C.§ 2709, the Fair Credit Reporting Act, 15 U.S.C. §§ 1681u and 1681v, and the Right to Financial Privacy Act, 12 U.S.C. § 3414(a)(5). Also delegates authority for certification of the necessity for non-disclosure of such national security letters and recertification of the necessity for non-disclosure of such national security letters under the afore-mentioned statutes.

Details: The USA Patriot Improvement and Reauthorization Act of 2005 (USAPA IRA) was enacted into law on March 9, 2006. It provides for procedural changes in the issuance of national security letters (NSLs). It provides that in order for the FBI to require that the recipient not disclose the fact of the request, the FBI must certify that certain harm may come were the request to be disclosed. If challenged more than one year later, the FBI must recertify that certain harm may come were the request to be disclosed. Further, the USAPA IRA provides that the NSL recipient may also challenge the receipt of the NSL itself. On the other hand, the FBI now has explicit enforcement authority and contempt penalties that attach to unlawful noncompliance with the NSL.

Specifically, the USAPA IRA provides, with respect to each of the NSL statutes set forth above, that a non-disclosure requirement attaches to the NSL "[i]f 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, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of a person." Once such a certification is made, if unchallenged, neither the recipient "or officer, employee, or agent of [such recipient] shall disclose to any person (other than those to whom disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request)" that the FBI has sought or obtained access to the records.[1]

There is a second non-disclosure certification provided by the USAPA IRA. If there is a challenge to the non-disclosure provision one year or more after the request is made, the Director or his designee, as defined above, may terminate the nondisclosure requirement or recertify that disclosure may result in the harm enumerated above.[2]

Thus, via this EC, I am delegating the authority to make the initial non-disclosure certification and any necessary subsequent non-disclosure recertification. However, in order to assure consistency between the persons to whom the non-disclosure certifications are delegated and the persons to whom signature authority is delegated, I am also revisiting the issue of the personnel to whom signature authority for NSLs has been delegated.

Since the enactment of the 2001 USA Patriot Act, which expanded the scope and availability of national security letters, I have issued several Electronic Communications delegating signature authority for such investigative tools. In light of the reorganization of the FBI, and specifically, the creation of the National Security Branch, it has become necessary to revise

---

[1] The language in the USPAP IRA with respect to each of the NSL statutes is identical, accounting for the different recipients, except that the language in the 1681v NSL statute applies to government agencies which conduct international terrorism investigations, rather than only the FBI, and the designee provision simply states that the government agency head or his designee may certify the danger that would arise from disclosure. It does not otherwise place any restrictions on the agency head's designee. However, for purposes of consistency, the non-disclosure certification delegation for 1681v will be made at the same level as the non-disclosure certification delegations for the other NSL statutes.

[2] There is also a provision under which, if a challenge to the non-disclosure provision is filed within one year of the request, a certification by the Director of the FBI will be treated as conclusive unless the court finds that the certification was made in bad faith.

those delegations in order to assure that all persons with legal authority to sign NSLs have in fact been delegated such authority. Moreover, it also makes sense to have all such delegations consolidated into one document.

Thus, the following delegations are being made for purposes of providing signature authority for NSLs and also providing the authority to initially certify as to the necessity for non-disclosure of the NSL request and the authority to recertify if the non-disclosure provision is challenged one year or more after the request. Most of the signature delegations already are in effect, while those that are created by this EC will be so noted. Nonetheless, this EC provides an exhaustive list of all of those FBI persons with NSL signature authority and non-disclosure certification and non-disclosure recertification authority.[3]

Thus, as now permitted by ECPA, the FCPA, and the RFPA, I hereby delegate certification signature authority, non-disclosure certification authority and non-disclosure recertification authority for NSLs to the following FBI Officials:

1. The Deputy Director;

2. The Executive Assistant Director for the National Security Branch;[4]

3. The Assistant Executive Assistant Director for the National Security Branch;

[3] This EC consolidates, and to the extent set forth below, revises, the delegations that took effect pursuant to the following ECs: 66F-HQ-A1255972, Serial 15, 66F-HQ-A1255972, Serial 31; 66F-HQ-A1255972, Serial 33; and 66F-HQ-A1255972, Serial 35. The EC, 66F-HQ-A1255972, Serial 33, providing for delegation of signature authority to The Senior Counsel for National Security Affairs is hereby rescinded, as that position no longer exists. Those portions of 66F-HQ-A1255972, Serials 31 and 35, which delegate signature authority to the Executive Assistant Director for Counterterrorism/Counterintelligence, are hereby rescinded, as that position no longer exists.

[4] The delegations of signature authority to the Executive Assistant Director and the Assistant Executive Assistant Director for the National Security Branch are new delegations, as those positions have just recently been created.

4. The Assistant Directors and all Deputy Assistant Directors of the Counterterrorism, Counterintelligence,[5] and Cyber Divisions;[6]

5. The General Counsel and Deputy General Counsel for the National Security Law Branch;[7]

6. The Assistant Director in Charge, and all SACs of the New York, Washington D.C., and Los Angeles field offices; and

7. The SACs in all other field divisions.

The NSLB is hereby authorized to issuance guidance with respect to the revision of the national security letter statutes, as well as the other changes encompassed by the USAPA IRA. One point should be made here, however. The signature authority, the initial non-disclosure certification authority, and the non-disclosure recertification authority are separate authorities. Because an NSL warrants signature does not necessarily mean that it warrants inclusion of a non-disclosure provision. Because an NSL once warranted a non-disclosure provision does not mean that one year later, it continues to warrant a non-disclosure provision. Such certifications should not and may not be made in a perfunctory manner. There must be an assessment by the individual who signs the NSL that there is a genuine need for non-disclosure because one of the enumerated dangers may arise from disclosure.

---

[5] The Counterintelligence Division was denoted in its previous signature delegation by its prior incarnation, as the National Security Division. See 66F-HQ-A1255972, Serial 15. This delegation brings its designation terminology up to date.

[6] While Counterintelligence Division and Cyber Division personnel are being given signature and non-disclosure certification and recertification authority for all NSLs, it is expected that they would rarely exercise that authority in the case of 1681v NSLs (which signature authority they have not had to date), which are limited to use in international terrorism investigations. It is possible, although not likely to be a frequent occurrence, that a counterintelligence or Cyber case may have an international terrorism aspect to it that would justify the issuance of a 1681v NSL.

[7] The Deputy General Counsel for the National Security Law Branch was denoted in its previous signature delegation by its prior incarnation, as Deputy General Counsel for National Security Affairs. See 66F-HQ-A1255972, Serials 15, 31. This delegation brings its designation terminology up to date.

To: All Divisions From: OGC
Re: , 03/9/2006

LEAD:

Set Lead 1: (adm)

ALL RECEIVING OFFICES

Disseminate to personnel involved in CI, IT, and Cyber operations and to other personnel as appropriate.

(Rev 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 03/09/2007

To: All Divisions **Attn:** ADs
DADs
SACs
ADICs
ASACs
CDCs

From: Records Management
RPAS/5334
Contact: Debbie O'Clair, 202-[redacted] b2

Approved By: Hooton William L
Caproni Valerie E

Drafted By: OClair Debra Anne

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-06-2007 BY 65179/DMH/KSR/RW

Case ID #: 319W-HQ-A1487699-RMD 1076786

Title: PROCEDURAL AND OPERATIONAL ISSUANCES -
RECORDS MANAGEMENT DIVISION (RMD)

Synopsis: Provides immediate interim guidance related to records management of National Security Letters (NSL).

Details: The below guidance is provided as an immediate interim solution to the proper recording of NSLs.

Original signed NSLs are to be sent to the recipient. Record copies of the NSLs are to be uploaded in the investigative case file using one of the following new document types:

NSLTSI (NSL Telephone Subscriber Information)
NSLTTR (NSL Telephone Toll Records)
NSLESI (NSL Email Subscriber Information)
NSLETR (NSL Email Transactional Records)
NSLFR (NSL Financial Records, RFPA Section 3414(a)(5))
NSLFIL (NSL Financial Institutional Listings, FCRA 1681u(a))
NSLCII (NSL Consumer Identifying Information, FCRA 1681u(b))
NSLFCR (NSL Full Credit Report, FCRA 1681v)

Effective Monday, March 12, 2007, modifications to the Automated Case Support (ACS) will have been completed to allow the entry of the above document types when uploading NSLs within ACS. Offices are to advise and assist those employees who upload NSLs in identifying the appropriate document type for each NSL. Offices are also to advise employees to use the originating

(issuing) office of the NSL in the "From" field when uploading the NSL to ACS. For example if the Tampa Field Office SAC signs off issuing an NSL for a Miami Field Office investigative case, the "From" field in ACS should indicate Tampa even though the Office of Origin is Miami.

In addition, reporting capability will be available within the next several weeks which will allow offices to generate reports of NSLs created by office, within a specified date range to facilitate statistical reporting.

It should be noted this is an interim immediate solution. Records Management Division (RMD) will host a working group of Headquarters and field personnel on Wednesday, March 14, 2007, to develop a permanent solution which minimizes human error and provides the necessary statistical reporting required. Offices are invited to nominate names of conversant and well-informed participants to attend this working group or participate via video teleconference to RMD Assistant Section Chief, Debbie O'Clair (via email). It is not mandatory to nominate an employee, and to ensure the working group is maintained at a reasonable number, not every nominated employee may be selected, but RMD seeks to ensure that the most affected stakeholders in this issue, the field offices, are represented in devising a resolution to this issue that is satisfactory to all.

To: All Divisions From: Records Management
Re: 319W-HQ-A1487699-RMD, 03/09/2007

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

Implement use of new NSL document types within ACS, assist and advise NSL records personnel in using the appropriate NSL document type for each document and to use issuing office of the NSL in the "From" field in ACS.

♦♦

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 04/07/2006

To: All Divisions

From: Office of the General Counsel
Contact: [redacted] (202) 324-[redacted]

Approved By: Caproni Valerie E
Thomas Julie F

b6
b7C
b2

Drafted By: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-06-2007 BY 65179/DMH/KSR/RW

1076786

Case ID #: 319X-HQ-A1487720-OGC

Title: (U) USA PATRIOT ACT RENEWAL - NEW LEGISLATIVE CHANGES TO FCI/IT LEGAL AUTHORITIES.

Synopsis: (U) Summarizes recent changes to national security legal authorities as a result of the "USA PATRIOT Improvement and Reauthorization Act of 2005 (Public Law 109-177) and the "USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006" (Public Law 109-178), and describes the preliminary implementation procedures.

Details: The President signed the "USA PATRIOT Improvement and Reauthorization Act of 2005" (USA PATRIOT IRA) and the "USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006" on March 9, 2006. The USAPA IRA makes permanent many of the sunseting provisions of the USA PATRIOT Act.[1] Additionally, both laws make significant changes to many national security legal authorities, including National Security Letters (NSLs) and certain FISA-related provisions, and impose new reporting requirements. Moreover, the new laws make changes in several substantive criminal laws, some of which may have implications in national security investigations.

The National Security Law Branch of the Office of General Counsel is issuing preliminary guidance on those portions of the two laws relating to national security operations. The following summarizes authorities contained in sections of the bills, to include 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] The USA PATRIOT Act refers to the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001," which was signed into law on October 26, 2001.

The USA PATRIOT Act Improvement and Reauthorization Act of 2005 is organized into the seven titles. Title I, which carries the same title as the overall bill, contains the significant changes to the FBI's national security tools.[2] Titles II through VII contain several other Acts and miscellaneous provisions:

- **Title I - USA PATRIOT Improvement and Reauthorization Act**

  Title I makes most of the original sunset provisions of the original USA PATRIOT Act permanent, though it creates new sunsets for the authorities in section 206 (FISA roving authority) and section 215 (FISA access to business records) of the USA PATRIOT Act, and section 6001 (Lone Wolf provision) of the Intelligence Reform and Terrorism Prevention Act of 2004. It also extends the duration of several FISA tools. Additionally, it makes significant changes to the National Security Letter statutes. Finally, the USAPA IRA requires new Congressional reporting of the use of national security tools.

- **Title II - Terrorist Death Penalty Enhancement**

  This portion of the USAPA IRA entitled the "Terrorist Death Penalty Enhancement Act of 2005" makes adjustments to the death penalty procedures for federal cases, including certain air piracy cases.

- **Title III - Reducing Crime and Terrorism at America's Seaports Act of 2005**

  This Title amends certain criminal statutes to strengthen maritime and seaport safety.

- **Title IV - Combating Terrorism Financing Act of 2005**

  This Title increases the penalties for terrorism financing, and adds new terrorism-related provisions to the specified unlawful activities that serve as money laundering predicates (including operating an illegal money transmitting business, such as the common "hawala" network).

- **Title V - Miscellaneous Provisions**

  As recommended by the WMD Commission, this Title creates a National Security Division within the U.S. Department of Justice, which is to be led by an Assistant Attorney General for National Security.

---

[2] Congress drafted the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 after the USA PATRIOT Improvement and Reauthorization Act of 2005. Congress used the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 to make additional adjustments to the nondisclosure provisions of FISA Business Records and National Security Letters contained in the USA PATRIOT IRA, and to add the "Privacy Protections for Library Patrons."

- **Title VI - Secret Service Authorization and Technical Modification Act of 2005**

  As the Title suggests, it modifies certain authorities of the Secret Service.

- **Title VII - Combat Methamphetamine Epidemic Act of 2006**

  This Title creates regulations for the control of precursor chemicals and enhances the criminal penalties for methamphetamine production.

TITLE I - USA PATRIOT IMPROVEMENT and REAUTHORIZATION ACT of 2005.

This EC will not address the new sections of the USAPA IRA in sequence; instead, the sections will be organized by national security tools.

SUNSET PROVISIONS

Sec. 102. USA PATRIOT Act Sunset Provisions.

Section 102 repeals section 224 of the USA PATRIOT Act, making most of the original sunset provisions permanent. This section adopts a new 4-year sunset (December 31, 2009) for sections 206 (roving authority) and 215 (business records) of the USA PATRIOT Act. The now permanent provisions of the USA PATRIOT Act are the following:

USA PATRIOT Act 2001 Provision	Description of Provision
Sections 201 & 202	Expanded Title III predicates.
Section 203(b) & (d)	Information sharing of foreign intelligence obtained in Title III and criminal investigations.
Section 204	Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral and Electronic Communications.
Section 207	Extended duration of certain FISAs.
Section 209	Seizure of voice mail with a search warrant.
Section 212	Emergency disclosures of e-mail and records by ISPs.
Section 214	FISA pen/trap authority.
Section 217	Interception of computer trespasser communications.
Section 218	Change in the probable cause ("significant purpose") standard of FISA.
Section 220	Nationwide search warrants for electronic evidence.

Section 223	Civil liability for certain unauthorized disclosures.
Section 225	Immunity for compliance with FISA wiretap.

Procedural Changes: None at this time. If necessary, additional guidance may be issued in the future.

Provision	New Sunset Date
FISA Roving Authority	December 31, 2009
FISA Business Records Authority	December 31, 2009

Sec. 103. Extension of Sunset Relating to Individual Terrorists as Agents of a Foreign Power.

Section 6001(b) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) addressed the "lone wolf" terrorist by broadening the definition of the "agent of a foreign power" for any person other than a United States person to include a person who "engages in international terrorism or activities in preparation thereof." The USAPA IRA extends the sunset of this provision 4 years (until December 31, 2009).

Procedural Changes: None at this time. If necessary, additional guidance may be issued in the future.

Provision	New Sunset Date
FISA "Lone Wolf"	December 31, 2009

FISA DURATION CHANGES

Sec. 105. Duration of FISA Surveillance on Non-United States Persons under Section 207 of the USA PATRIOT Act.

Section 105 extends the duration of both initiations and renewals of electronic surveillance (FISA § 105(e)), physical search (FISA § 304(d)), and pen register/trap and trace surveillance (FISA § 402(e)) for agents of a foreign power who are not U.S. persons.

Procedural Changes Related to the New FISA Durations: DOJ Office of Intelligence Policy and Review will implement these changes to the FISA process. The new durations for non-United States persons are reflected in the chart below. Overall, the new durations should translate into considerable savings in FBI and OIPR resources.

FISA Technique	Non-USP Initiations	Non-USP Renewals
Electronic Surveillance	120 days	1 year
Physical Search	120 days	1 year
Pen register/trap and trace	1 year	1 year

The initiations and renewals for United States persons will remain the same.

FISA Technique	USP Initiations	USP Renewals
Electronic Surveillance	90 days	90 days
Physical Search	90 days	90 days
Pen register/trap and trace	90 days	90 days

FISA BUSINESS RECORD CHANGES[3]

Sec. 106. Access to Certain Business Records Under Section 215 of the USA PATRIOT Act.

Section 106 makes the following changes to Sections 501 and 502 of the Foreign Intelligence Surveillance Act (FISA) regarding access to 215 Business Records.

Procedural Changes Related to FISA Business Records: FISA Business Records, which have been the subject of much debate, have been modified to contain more safeguards to protect civil liberties and privacy. These safeguards include special procedures and approvals for certain types of tangible things (i.e., library records), a directive to develop "minimization procedures," the recipient's right to seek judicial review of an order, and a recipient's right to disclose an order for the purpose of obtaining legal advice or for assistance in complying with the order. The following charts summarize significant provisions in the new law.

Scope of FISA Business Records authority.	• This authority may be used to obtain "**any tangible things (including books, records, papers, documents, and other items).**" This authority is broad, similar in scope to a criminal grand jury subpoena. • This authority requires additional procedures for certain special categories of records (see below).

[3] The changes included in this section also include the changes made by section 3 and 4 of the "USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006."

Special Categories of Tangible Things	Congress designated particular categories of records for special procedures and approvals. The FBI will adjust procedures to account for the special designation.
• Special Categories:	Library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, and medical record containing information that would identify a person.
• Approval Level for special categories:	The Director of the FBI may delegate the authority to either – • the **Deputy Director** of the FBI; or • the **Executive Assistant Director (EAD) for National Security** (or any successor position). **No further delegation is allowed.**
• Congressional Oversight of special categories:	Attorney General must provide annual report (April) to the House Judiciary Committee (HJC), the House Permanent Select Committee on Intelligence (HPSCI), the Senate Judiciary Committee (SJC), and the Senate Select Committee on Intelligence (SSCI). • Number of FISA business record orders granted, modified, or denied for the special categories of tangible things.

FISA Business Record Standard- **Relevance:**	The FBI's facts must show that there are "reasonable grounds to believe that the tangible things sought are **relevant to an authorized investigation.**"
• Presumptive Relevance Test:	The tangible things are presumptively relevant if the facts show they pertain to – "(i) a foreign power or an agent of a foreign power; (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigations..."

FISA Business Record Order:	• The order must describe the tangible things with **sufficient particularity** to permit them to be fairly identified. • **Date for return** - the order will contain a date on which the tangible things must be provided. • Recipient must have a **reasonable period of time** to produce. • The Order may only require production of tangible things that would be available with a grand jury subpoena or a District Court order (in other words, privileges under the law will apply to Business Record orders).

FISA Business Record Non-Disclosure Provision:	No person shall disclose the fact that the FBI has sought tangible things.
• Exceptions to non-disclosure:	A recipient may disclose a FISA Business Record Order to – (1) persons to whom disclosure is necessary to comply; (2) an attorney to obtain legal advice or assistance with respect to the production; (3) a person as permitted by the FBI Director (or designee).
• Extension of nondisclosure to others:	• If the recipient discloses to another person (see exceptions above), the recipient shall notify the person of the nondisclosure requirement. • The person to whom disclosure is made shall be subject to the nondisclosure requirement. • The FBI director (or designee) may ask the recipient to identify the other persons to whom disclosure of the Business Record order will be made (**except that the recipient does not have to identify the attorney**).

Judicial Challenge of FISA Business Record authority:	The recipient of a FISA Business Record order may challenge the legality of the order in the Foreign Intelligence Surveillance Court.
• Challenging the order:	• Recipient may move to modify or set aside the order. • FISC may grant the motion only if the order does not meet the requirements of FISA or is otherwise unlawful.

• Challenging the non-disclosure provision:	• Not less than 1 year after the order, the recipient may move to modify or set aside the nondisclosure order. • FISC may grant such a motion only if there is no reason to believe that disclosure may endanger the national security of the U.S., interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person. • The FISC will treat as conclusive a **certification** by the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the FBI that a disclosure may endanger the national security of the U.S. or interfere with diplomatic relations.
• Security:	• Filings shall be under seal •Chief Justice of the U.S., in consultation with the AG and the DNI, will establish security measures.

Minimization Procedures for FISA Business Records:	Within 180 days of enactment, the Attorney General **shall** adopt specific minimization procedures governing the **retention** and **dissemination** of FISA Business Record information.
•U.S. Person information:	The minimization procedures should minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting U.S. persons consistent with the U.S. intelligence community need to obtain, produce and disseminate foreign intelligence information.
• Evidence of a crime:	The procedures should allow for the retention and dissemination of information that is evidence of a crime.

Procedural Changes Related to Congressional Oversight of FISA Business Records: The new law beefs up the Congressional reporting requirements for the FISA Business Record authority. OIPR will have the responsibility for reporting the FISA Business Record statistics to Congress.

Reporting Cycle:	Attorney General will report on an annual basis (April of each year).
Congressional Committees:	•House Permanent Select Committee on Intelligence •House Judiciary Committee •Senate Select Committee on Intelligence •Senate Judiciary Committee

Reporting Categories:	(1) Total number of applications for FISA Business Records. (2) Total number of orders granted, modified, or denied. (3) Total number of orders granted, modified, or denied for the special categories of tangible things. • Library circulation records, library patron lists, book sales records, or book customer lists. • Firearms sales records. •Tax return records. •Educational records. • Medical records containing information that would identify a person.
Additional unclassified report:	Annually (April of each year), the Attorney General shall make an unclassified report on the total number of FISA Business Records applications, and the total number of orders granted, modified, or denied.

Sec. 106A Audit on Access to Certain Business Records for Foreign Intelligence Purposes.

Section 106A directs the Inspector General of the Department of Justice to perform a comprehensive audit of the effectiveness and use, including improper or illegal use, of the FISA Business Records authority. The audit will take place in two phases, covering the years of 2002 to 2006.

Procedural Changes Related to the Audit of FISA Business Records: The Inspector General's Office of the Department of Justice (DOJ IG) started the audit process in January 2006, in anticipation of the new USA PATRIOT Improvement and Reauthorization Act. It will be incumbent upon the FBI to cooperate with the DOJ IG to complete the two-phased audit. Per established procedures, the FBI's Inspection Division will be the primary point of contact for the DOJ IG. Additional guidance may be published as the audit process continues.

Scope of Audit:	The IG will perform a comprehensive audit of the effectiveness and use, including any improper or illegal use, of the investigative authority.
Timing of Audit:	For 2002, 2003, and 2004, the audit should be completed within one year of enactment (March 9, 2007).
	For 2005 and 2006, the audit should be completed by December 31, 2007.
Report results to Congress:	The IG shall submit the audit reports to – • House Judiciary Committee. • House Permanent Select Committee on Intelligence. • Senate Judiciary Committee. • Senate Select Committee on Intelligence.

Examine effectiveness of the tool:	Audit will look at the following for effectiveness – • Categories of records obtained. • The importance to the FBI and the IC of the information obtained. • The manner in which the information is collected, retained, analyzed, and disseminated by the FBI (this will include an examination of the access to "raw data" provided by the FBI to other agencies of the Federal, State, local, or tribal governments, or private sector agencies). • The minimization procedures adopted by the AG. • Whether, and how often, the FBI used information to produce analytical intelligence products for the FBI, the IC, or other Federal, State, local, or tribal government agencies. • Whether, and how often, the FBI provided the information to law enforcement authorities for criminal proceedings.
Examine the process:	The audit process will look at the following: • How often the FBI requested DOJ to submit an application and the request was not submitted to the court (including the basis for the decision). • Whether the court granted, modified, or denied the application. • The justification for the failure of the AG to issue implementing procedures governing the requests in a timely fashion, including whether the delay harmed national security. • Whether bureaucratic or procedural impediments prevent the FBI from fully using the authority.

FISA ROVING SURVEILLANCE CHANGES

Sec. 108. Multipoint Electronic Surveillance Under Section 206 of the USA PATRIOT Act.

This section modifies FISA sections 104(a) and 105(c), to clarify the amount of detail the FBI must provide to obtain a FISA roving surveillance order.

Procedural Changes Related to FISA Roving Surveillance:

The application must now include a description of the "specific" target when the target is identified by description rather than by name. The section also adds a return requirement on the FBI in national security investigations. This is consistent with Congress' intent to provide an extra layer of judicial review and to prevent the potential abuse of this investigative authority.

OIPR will implement the new requirements for the FISA roving surveillance. OIPR and FBI OGC may develop more specific guidance on the new process for obtaining this authority in the future.

Standard for roving surveillance:	• The FISC must find the possibility of the target thwarting surveillance based upon specific facts. • The order must describe the specific target in detail when authorizing a roving surveillance for a target whose identity is not known.

Return requirement:	•Presumed **10 day notice** – the FBI (applicant) must provide notice to the court within 10 days unless the court finds good cause to justify a longer period of up to 60 days.
	The FBI must inform the court: • The nature and location of new facility. • The facts and circumstances relied upon by applicant. • Any new minimization procedures. • The total number of electronic surveillances that have been or are being conducted under the roving authority.

Consistent with Congress' intent to provide more oversight, the reporting requirements for FISA roving surveillance have been changed.

Procedural Changes Related to FISA Roving Surveillance Congressional Oversight: OIPR will maintain responsibility for reporting on the FISA roving surveillance.

Reporting cycle:	The Attorney General will report on a semi-annual basis.
Congressional Committees:	• House Permanent Select Committee on Intelligence • Senate Select Committee on Intelligence • Senate Judiciary Committee
Reporting categories:	• Total number of applications made for orders and extensions. • Each criminal case in which information has been authorized for use at trial, during the period covered by such report. • Total number of emergency employments and total number of subsequent orders approving or denying surveillance.

FISA OVERSIGHT CHANGES

In section 109 of the USA PATRIOT Act Improvement and Reauthorization Act, Congress has implemented additional reporting requirements for the use of FISA physical search authority and FISA pen registers and trap and trace authority. This section modifies the reporting requirements in FISA sections 306 and 406(b).

Congressional Reporting on FISA Physical Search authority:

Reporting cycle:	Attorney General will report on a semiannual basis.
Congressional Committees:	• House Permanent Select Committee on Intelligence • House Judiciary Committee • Senate Select Committee on Intelligence • Senate Judiciary Committee
Reporting categories:	Report the following regarding emergency physical searches – • Total number of applications. • Total number of orders granted, modified, or denied. • Number of physical searches involving the residences, offices, or personal property of U.S. persons, and the number of occasions the AG provided notice. • Total number of emergency authorizations, and total number of subsequent orders approving or denying the physical searches.

Congressional Reporting on FISA Pen Register and Trap and Trace authority:

Reporting cycle:	Attorney General will report on a semiannual basis.
Congressional Committees:	• House Permanent Select Committee on Intelligence • House Judiciary Committee • Senate Select Committee on Intelligence • Senate Judiciary Committee
Reporting categories:	Report the following regarding pen registers/trap and trace – • Total number of applications. • Total number of orders granted, modified, or denied. • Total number of emergency authorizations, and total number subsequent orders approving or denying the pen registers/trap and trace.

Procedural Changes Related to Enhanced Congressional Oversight: If necessary, OIPR and FBI OGC will publish guidance in response to the new provisions. OIPR will retain responsibility for reporting to Congress on FISA related activities.

FISA PEN REGISTER/TRAP AND TRACE CHANGES

Sec. 128. PATRIOT Section 214; Authority for Disclosure of Additional Information in Connection with Orders for Pen Register and Trap and Trace Authority under FISA.

Congress modified the FISA pen register and trap and trace devices authority to give the FBI access to more information through this authority. The pertinent portion of the new statute describing the information available to the FBI is reproduced here (highlights added):

> FISA § 402 [50 U.S.C. § 1842]. Pen registers and trap and trace devices for foreign intelligence and international terrorism investigations.

(C) shall direct that, upon the request of the applicant, the provider of a wire or electronic service shall disclose to the Federal officer using the pen register or trap and trace device covered by the order –

(i) in the **case of the customer or subscriber using the service covered** by the order (for the period specified by the order) –

(I) the **name of the customer or subscriber**;
(II) the **address of the customer or subscriber**;
(III) the **telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission information**;
(IV) the **length of the provision of service** by such provider to the customer or subscriber and the **types of services** utilized by the customer or subscriber;
(V) in the case of a provider of local or long distance telephone service, any **local or long distance telephone records of the customer** or subscriber;
(VI) if applicable, any **records reflecting period of usage (or sessions)** by the customer or subscriber; and
(VII) any **mechanisms and sources of payment** for such service, including the number of any credit card or bank account utilized for payment for such service; and

(ii) if available, with respect to **any customer or subscriber of incoming or outgoing communications to or from the service covered** by the order –

(I) the **name of such customer or subscriber**;
(II) the **address of such customer or subscriber**;
(III) the **telephone or instrument number, or other subscriber number or identifier, of such customer or subscriber, including any temporarily assigned network address or associated routing or transmission information**; and
(IV) the **length of the provision of service** by such provider to such customer or subscriber and the **types of services** utilized by such customer or subscriber.

The chart below summarizes the information available through the new adjustments to the FISA tool.

Customer/subscriber using the service covered:	Information available through PR/TT: • Name of the customer or subscriber. • Address of the customer or subscriber. • Telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission information. • Length of service. • Types of service. • Any local or long distance telephone records of the customer/subscriber. • Records reflecting period of usage. • Mechanisms/sources of payment, including the number of any credit card or bank account used.
Customer/subscriber of incoming or outgoing communications to/from the service covered:	Information available through PR/TT: • Name of customer/subscriber. • Address of customer/subscriber. • Telephone or instrument number, or other subscriber number or identifier, ... including any temporarily assigned network address or associated routing or transmission information. • Length of service. • Types of service.

The chart below summarizes the Congressional reporting requirements for the use of the FISA pen register and trap and trace authority.

Reporting cycle:	Attorney General shall report on a semiannual basis.
Congressional Committees:	• House Permanent Select Committee on Intelligence • House Judiciary Committee • Senate Select Committee on Intelligence • Senate Judiciary Committee
Reporting categories:	Use of pen registers and trap and trace.

Procedural Changes Related to Pen Registers/Trap and Trace: OIPR will retain the reporting responsibilities for the FISA pen register/trap and trace authority.

The FBI will now be able to obtain subscriber information (including billing information) with a FISA pen register/trap and trace, without having to couple the request with a FISA Business Record request. This provision should make this investigative tool more useful to

the FBI. OIPR has already made the changes to its pen register/trap and trace format to take advantage of the new provision.

EMERGENCY DISCLOSURES

Sec. 107 Enhanced Oversight of Good-Faith Emergency Disclosures Under Section 212 of the USA PATRIOT Act.

The emergency disclosure provision, codified at 18 U.S.C. § 2702(b)(8) & (c)(4), provides law enforcement with the ability to gain quick access to e-mail content and records under emergency conditions. The USA PATRIOT Act created the emergency disclosure provision which explicitly permits, but does not require, a service provider (most often an ISP) to voluntarily disclose to law enforcement information, including e-mail content, in emergencies involving a risk of death or serious physical injury. Such disclosures are outside of the compulsory process – subpoena, court order, and search warrant – that is generally required before law enforcement can obtain such information from a service provider. See, 18 U.S.C. § 2703.

Section 107 makes changes to the emergency disclosure provision of 18 U.S.C. Section 2702, including the requirement for more Congressional reporting, to deal with the concern that this authority was not subject to sufficient Congressional, judicial or public oversight.

Procedural Changes Related to Good-Faith Emergency Disclosures: The Attorney General must now report annually to Congress on the number of accounts subject to disclosure, and the Attorney General must report the basis for the voluntary disclosures in investigations that are closed without filing criminal charges.

The FBI will need to track the use of this investigative authority for reporting purposes. The FBI will publish additional guidance on this issue as necessary.

Voluntary disclosure by provider:	If the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay.
Reporting cycle:	Attorney General shall report on an annual basis.
Congressional Committees:	• House Judiciary Committee • Senate Judiciary Committee
Reporting categories:	• Number of accounts from which voluntary disclosures were received. • Summary of the basis for disclosure where the investigation was closed without criminal charges.

NATIONAL SECURITY LETTERS[4]

Sec. 115. Judicial Review of National Security Letters.

Title 18, Chapter 223 of the United States Code (Witnesses and Evidence) is amended to include a new section 3511 which provides for the judicial review of NSLs.

Procedural Changes Related to the Judicial Review of NSLs: This new section modifies the NSL authorities under the Electronic Communications Privacy Act (ECPA)(18 U.S.C. § 2709), the Fair Credit Reporting Act (FCRA)(15 U.S.C. § 1681u and 15 U.S.C. § 1681v), and the Right to Financial Privacy Act (RFPA)(12 U.S.C. § 3414), to make it clear that the recipient may seek the help of an attorney, and may challenge the legality of an NSL order and its non-disclosure provision in Federal District Court. A Federal District Court can modify or set aside an NSL if it is unreasonable, oppressive, or otherwise unlawful. It continues to be important for the FBI to serve NSLs only if the information sought falls within the statutory categories, and which are not overly broad or oppressive.

Future practice will give the FBI an idea of how many NSL challenges can be expected in a calendar year. If Federal grand jury practice is any indication, the number of NSLs challenged on a yearly basis should be small. Regardless, the FBI Field Office will need to work with local Assistant United States Attorneys when a recipient challenges the legality of an NSL or the non-disclosure provision. Additionally, FBI Field Offices should immediately notify FBI OGC if they receive notice of any challenge to an NSL or the NSL's nondisclosure provision. The following chart breaks down the new provisions (including jurisdictional issues).

The new law also gives the U.S. government a mechanism to address the situation where a recipient fails to comply with the NSL, which has been missing from the investigative tool in the past. Again, this procedure will require the assistance of a local United States Attorney's Office.

Judicial review of NSL (Recipient may challenge the request):	• Jurisdiction: In the U.S. District in which the recipient resides or does business.
	• Recipient may ask court to set aside or modify request.
	• Court will grant the recipient's motion if the NSL is **unreasonable, oppressive, or otherwise unlawful.**

[4] The changes listed in this section also include the changes made by sections 4 and 5 of the "USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006."

Judicial review of NSL nondisclosure provision (Recipient may challenge the nondisclosure provision):	• Jurisdiction: In the U.S. District in which the recipient resides or does business.
	• Filed **within one year** of NSL request – • Court may **modify/set aside** the non-disclosure if... "no reason to believe that disclosure may endanger the national security of the U.S., interfere with criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person." • **Certification/Authority level**: Court will treat as conclusive the certification by the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the FBI that disclosure may endanger the national security of the United States or interfere with diplomatic relations (unless made in bad faith).
	• Filed **one year or more** after the NSL – • Within 90 days of recipient's petition, designated government officials must either **terminate** the nondisclosure requirement or **recertify** that the disclosure "may result in a danger to the national security of the U.S., interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person." • **Termination/Recertification Authority level**: The Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the FBI, or his designee in a position not lower than Deputy Assistant Director at FBI headquarters or a SAC in an FBI field office designated by the Director shall either terminate the nondisclosure requirement or recertify that disclosure "may result in a danger to the national security of the U.S., interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person." • **Conclusive**: Certification by the AG, DAG, an Assistant Attorney General, or the Director of the FBI that disclosure may endanger the national security of the United States or interfere with diplomatic relations shall be treated as conclusive (unless made in bad faith).

Failure to Comply:	• The Attorney General may invoke the aid of a Federal District Court. • Jurisdiction: U.S. District in which the investigation is carried on, or the person or entity resides or does business or may be found. • Court may compel by ordering person/entity to comply. • Failure to obey is punishable by contempt.

Court Proceedings & Security:	• Court must close hearings to the extent necessary to prevent an unauthorized disclosure of NSL. • Petitions, filings, records, orders, and subpoenas must be kept **under seal** to the extent and as long as necessary to prevent unauthorized disclosure. • At government's request, ex parte and in camera review of government's submissions which may contain classified material.

Sec. 116. Confidentiality of National Security Letters.

Section 116 makes changes to the National Security Letter authorities contained in the Electronic Communications Privacy Act (ECPA) (18 U.S.C. § 2709), the Right to Financial Privacy Act (RFPA)(12 U.S.C. § 3414), and the Fair Credit Reporting Act (FCRA) (15 U.S.C. §§ 1681u and 1681v).

For example, Congress used this section to clarify the application of NSLs [18 U.S.C. § 2709 - telephone toll and transactional records] to libraries. A library is subject to an NSL only if it falls within the definition of a wire or communications provider.

Libraries and 18 U.S.C. § 2709 (telephone toll and transactional records):	A library is not a wire or electronic communications service provider unless the library is providing the services defined in 18 U.S.C. § 2510(15)(electronic communication service).

Additionally, this section is used to statutorily establish the NSL nondisclosure requirements and the exceptions to the nondisclosure requirement available to a recipient.

Procedural Changes Related to National Security Letters Confidentiality: To avoid overstepping this authority, the FBI should not issue an NSL to a library unless the library is acting as an internet service provider and not merely providing internet access to its customers through some other Internet service provider (e.g, AOL). If you have any questions regarding the application of this provision to a particular library, please direct your questions to FBI OGC NSLB.

The other significant changes to NSLs regarding confidentiality are common to all NSLs used by the FBI. In order to activate the nondisclosure requirement, the NSLs must contain a certification from the Director of the FBI, or a Special Agent in Charge in an FBI field office. This new legislation allows designation of this certification 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 must choose which offices needed, and were properly

prepared to exercise, the delegated authority. The Director has made delegations to FBI Field Offices in a separate communication. Field Offices with delegated authority will receive instructions on the process of preparing and issuing NSLs (instructions and updated forms will be posted on the FBI OGC National Security Law Branch website). The remaining changes are summarized in the chart below. FBI OGC NSLB will publish additional guidance on this authority as necessary.

Nondisclosure activated by FBI Certification:	• **FBI certification**: There may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, if a recipient discloses that the FBI has sought or obtained access to information or records under NSL statutes.
	• **Authority level: Director of the FBI,** or his designee in a position not lower than **DAD at FBI headquarters,** or a **Special Agent in Charge in a Bureau field office designated by the Director.**
Exceptions - Recipient may disclose NSL request:	• Recipient may disclose to persons necessary to comply with NSL request.
	• **Attorney**: Recipient may disclose to an attorney to obtain legal advice or legal assistance regarding any NSL request.
Notice:	• The NSL shall notify the recipient of the nondisclosure requirement.
	• Recipient disclosing NSL to an individual necessary to comply or, to an attorney, shall inform them of the applicable nondisclosure requirement.
FBI request for identity of persons to whom recipient plans to disclose NSL:	• Only activated at the request of the FBI Director or Director's designee.
	• Recipient of NSL shall identify the persons to whom disclosure will be made or was made.
	• **EXCEPT**: Nothing requires the person to identify an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance.

Sec. 117. Violations of Nondisclosure Provisions of National Security Letters.

This section makes it a federal crime for an individual to knowingly and with the intent to obstruct an investigation or judicial proceeding violate the nondisclosure provision of an NSL.

Procedural Changes Related to Violations of National Security Letter Non-disclosure: None at this point.

Obstruction of an Investigation (18 U.S.C. § 1510):	• Individual must have been notified of the nondisclosure provision.
	• Individual must knowingly and with the intent to obstruct an investigation or judicial proceeding violate the nondisclosure provision.
	• Punishable by up to five years imprisonment, a fine, or both.

Sec. 118. Reports on National Security Letters.

Section 118 of the USA PATRIOT Improvement and Reauthorization Act of 2005 outlines a new reporting scheme for National Security Letters.

Procedural Changes Related to National Security Letter Reporting: This section now requires that NSL statistics be reported to the House and Senate Judiciary Committees, in addition to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. Additionally, Congress has directed that the NSL requests made pursuant to the 15 U.S.C. § 1681v [Fair Credit Reporting Act] be reported semi-annually to the House Committee on Financial Services and the Senate Committee on Banking, Housing and Urban Affairs, in addition to the House and Senate intelligence committees. These provisions are consistent with Congress' desire for more oversight of the national security investigative tools. Finally, Congress has directed that the Attorney General provide an unclassified report annually (April) which will report the aggregate numbers of NSL requests concerning different U.S. persons. With the unclassified report, Congress intends for the public to have a better view of the material Congress sees in conducting its oversight responsibilities.

The FBI OGC's National Security Law Branch and OIPR will provide future guidance on the FBI's role in the reporting of NSLs.

Current NSL Reports:	• AG reports on a semi-annual basis.
	• Reports will now also be made to the House Judiciary Committee, the House Permanent Select Committee on Intelligence, the Senate Judiciary Committee, and the Senate Select Committee on Intelligence.

Enhanced Oversight of 15 U.S.C. § 1681v NSLs (for credit agency consumer records):	• AG reports on a semi-annual basis.
	• Reports will now also be made to the House Judiciary Committee, the House Committee on Financial Services, the House Permanent Select Committee on Intelligence, the Senate Judiciary Committee, the Senate Housing and Urban Affairs Committee, and the Senate Select Committee on Intelligence.

Aggregate Report of NSL requests:	• AG reports annually (April).
	• Total number of NSL (excluding NSL's for subscriber information) requests for information concerning different U.S. persons.
	• Unclassified report.

Sec. 119. Enhanced Oversight of National Security Letters.

Consistent with Congress' theme of more oversight, Congress has directed that the Inspector General of the Department of Justice shall perform an audit of the effectiveness and use, including any improper or illegal use, of national security letters issued by the Department of Justice.

Procedural Changes Related to the Audit of National Security Letters: This DOJ IG audit of the use of NSLs, which began in January of 2006, will require the cooperation of the FBI. Congress' goal in this audit is to obtain detail on the specific functions and characteristics of NSLs and an analysis of the necessity of this national security investigative tool. As with DOJ IG's audit of the FISA Business Record authority, the FBI's Inspection Division will be the primary point of contact for the DOJ IG (per established procedures). The FBI OGC NSLB may issue additional guidance as the audit process continues.

Requirements of DOJ IG Audit:	Comprehensive audit of – • Use of NSLs for 2003 through 2006. • Description of noteworthy facts/circumstances, including any improper or illegal use of NSLs.
Timing of Audit:	• For 2003 and 2004, must be completed not later than one year after enactment (March 9, 2007).
	• For 2005 and 2006, must be completed not later than December 31, 2007.
Congressional Committees:	• House Judiciary Committee and House Permanent Select Committee on Intelligence. • Senate Judiciary Committee and Senate Select Committee on Intelligence.

Examine Effectiveness of NSLs:	The audit will examine: • Importance of the information acquired by DOJ to the intelligence activities of DOJ and other members of the IC. • How information is collected, retained, analyzed, and disseminated (including access to raw data) to members of the IC community, and other Federal, State, local or tribal governments, or private sector entities. • How often NSL information was used to produce an analytical intelligence product for distribution to the IC community, and to other Federal, State, local or tribal governments. • Whether, and how often, NSL information was provided to law enforcement authorities for use in criminal investigations. • Following enactment of the USA PATRIOT IRA, the number of NSLs issued without the certification necessary to create a nondisclosure obligation. • Types of electronic communications and transactional information obtained under § 2709, and the procedures DOJ used if content information is obtained.

Feasibility of Minimization Procedures:	•Not later than February 1, 2007, or upon completion of the 2003/2004 audit, the Attorney General and the Director of National Intelligence shall jointly submit a report on the feasibility of applying minimization procedures to protect the constitutional rights of U.S. persons.
	• Report goes to the House Judiciary Committee, the House Permanent Select Committee on Intelligence, the Senate Judiciary Committee, and the Senate Select Committee on Intelligence.

DELAYED NOTICE SEARCH WARRANTS

Sec. 114. Delayed Notice Search Warrants.

The section changes the procedural requirements for the warrants and increases the oversight of the delayed notice search warrants (18 U.S.C. § 3103a). A major change is the implementation of a 30 day notice requirement, as opposed to the former requirement of "within a reasonable period" of the warrant's execution.

Procedural Changes Related to Delayed Notice Search Warrants: In applicable cases, the FBI (through the U.S. Department of Justice trial attorney or Assistant United States Attorney) must provide the facts to a court to show there is "reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse effect." The showing will have to be updated for each extension.

Notification Delay	No more than **30 days** (or a later date certain if facts justify). •undue delay of trial is not a basis for a delayed notice.
Extensions of Delays	**90 days** (unless the facts justify longer)-- •granted upon an updated showing of the need for further delay.
Reporting	Annual reporting to Congress by Court (starting with the fiscal year ending September 30, 2007).

OTHER LAW ENFORCEMENT/CRIMINAL RELATED PROVISIONS

Sec. 104. Section 2332b and the Material Support Sections of Title 18, United States Code.

This section makes permanent the material support of terrorism provisions in section 6603 of the Intelligence Reform and Terrorism Prevent Act of 2004 (18 U.S.C. §§ 2332b and 2339B).

Procedural Changes: None at this time. If necessary, additional guidance may be issued in the future.

Sec. 110. Attacks Against Railroad Carriers and Mass Transportation Systems.

This section merges wrecking trains (18 U.S.C. § 1992) and attacks on mass transit (18 U.S.C. § 1993) into one section - 18 U.S.C. § 1992. The new law expands the law to cover the planning for such attacks, so it is now a federal crime to surveil, photograph, videotape, diagram, or collect information as part of a plan for an attack.

Procedural Changes: None at this time. If necessary, additional guidance may be issued in the future.

Sec. 111. Forfeiture.

This section expands the authorization to confiscate property located within the United States when it constitutes proceeds used in or derived from trafficking in nuclear, chemical, biological, or radiological weapons technology or material.

Procedural Changes: None at this time. If necessary, additional guidance may be issued in the future.

Sec. 112. Section 2332b(g)(5)(B) Amendments Relating to the Definition of Federal Crime of Terrorism.

This section adds drug trafficking in support of terrorism (21 U.S.C. § 960A) and receiving foreign military-type training from a foreign terrorist organization (18 U.S.C. § 2339D) to the definition of federal crimes of terrorism (18 U.S.C. § 2332b(g)(5)(B)).

Procedural Changes: None at this time. If necessary, additional guidance may be issued in the future.

Sec. 113. Amendments to Section 2516(1) of Title 18, United States Code (Title III).

This section adds 20 federal crimes related to terrorism to the list of predicate offenses that may be used as a basis to intercept wire, oral, or electronic communications (18 U.S.C. § 2516(1)). The new wiretap predicates include the following:

- 18 U.S.C. § 37 [violence at international airports]
- 18 U.S.C. § 43 [animal enterprise terrorism]
- 18 U.S.C. § 81 [arson within special maritime and territorial jurisdiction]
- 18 U.S.C. §§ 175, 175b, and 175c [biological agents]
- 18 U.S.C. § 832 [nuclear and weapons of mass destruction threats]
- 18 U.S.C. § 842 [explosive materials]
- 18 U.S.C. § 930 [possession of weapons in Federal facilities]
- 18 U.S.C. § 956 [conspiracy to harm persons or property overseas]
- 18 U.S.C. § 1028A [aggravated identity theft]
- 18 U.S.C. § 1114 [killing or attempted killing of Federal employees, including any member of the uniformed services]
- 18 U.S.C. §1116 [killing or attempted killing of certain foreign officials, including internationally protected persons]
- 18 U.S.C. § 1992 [attacks on mass transit]
- 18 U.S.C. § 2340A [torture]
- 18 U.S.C. § 2339 [harboring terrorists]
- 18 U.S.C. § 2339D [receiving military-type training from a foreign terrorist organization]
- 18 U.S.C. § 5324 [structuring transactions to evade reporting requirements]
- 49 U.S.C. §46504 [assault on a flight crew member with a dangerous weapon]
- 49 U.S.C. §46505(b)(3) or (c) [weapons offenses on board an aircraft]

Procedural Changes: None at this time. If necessary, additional guidance may be issued in the future.

Sec. 122. Prohibition of Narco-Terrorism.

This section makes it a federal crime to engage in drug trafficking to benefit terrorism (amended the Controlled Substance Import and Export Act - 21 U.S.C. §§ 951 et seq.). To prove this crime, the evidence must show that a defendant had knowledge that the person or organization has engaged or is engaging in terrorism.

Procedural Changes: None at this time. If necessary, additional guidance may be issued in the future.

Sec. 123. Interfering with the Operation of an Aircraft.

This section makes it a federal crime to interfere with or disable a pilot or navigation facility operator with the intent to danger or with reckless disregard for human safety (e.g., aiming lasers at pilots) (18 U.S.C. § 32).

Procedural Changes: None at this time. If necessary, additional guidance may be issued in the future.

Sec. 124. Sense of Congress Relating to Lawful Political Activity.

Congress uses this section to express the sense of Congress that federal investigations should not be based solely upon an American citizen's membership in a non-violent political organization or their otherwise lawful political activity.

Procedural Changes: None at this time. All employees are reminded, however, that neither criminal nor national security investigations of U.S. persons may be predicated solely on the exercise of First Amendment rights.

Sec. 127. Sense of Congress.

Congress uses this section to express its sense that the victims of terrorist attacks should have access to the forfeited assets of terrorists under 18 U.S.C. § 981.

Procedural Changes: None at this time. If necessary, additional guidance may be issued in the future.

DATA-MINING ACTIVITIES

Sec. 126. Report on Data-Mining Activities.

This section requires the Attorney General to report to Congress on any Department of Justice (including the FBI) initiative that uses pattern-based data-mining or is developing pattern-based data-mining. Among several topics, the report is to explain how any pattern-based data-mining initiatives collect, review, gather, and analyze information, and how the initiatives will ensure the accuracy of information and protect the privacy and due process rights of individuals.

The statute defines pattern-based data-mining as follows in section 126(b)(1):

> (1) Data-Mining.——The term "data-mining" means a query or search or other analysis of one or more electronic databases, where——
>
> (A) at least one of the databases was obtained from or remains under the control of a non-Federal entity, or the information was acquired initially by another department or agency of the Federal Government for purposes other than intelligence or law enforcement;
>
> (B) the search does not use personal identifiers of a specific individual or does not utilize inputs that appear on their face to identify or be associated with a specified individual to acquire information; and
>
> (C) a department or agency of the Federal Government is conducting the query or search or other analysis to find a pattern indicating terrorist or other criminal activity.

Procedural Changes:

FBI will participate in preparing the report.

TITLE II - TERRORISM DEATH PENALTY ENHANCEMENT

Among several provisions, this Title adjusts the Sentencing Guidelines to create a term of post-incarceration supervision in connection with a conviction for a federal terrorism crime for any term of years or for life and makes legal counsel available for death-penalty defendants.

Procedural Changes Related to the Terrorism Death Penalty Enhancement: None at this time.

TITLE III - REDUCING CRIME AND TERRORISM AT AMERICA'S SEAPORTS ACT of 2005

This Title strengthens statutes related to seaport and maritime safety. For example, the Title prohibits the maritime transportation of weapons of mass destruction for use in a federal terrorism crime (18 U.S.C. § 2283). Additionally, it prohibits the maritime transportation of terrorists (18 U.S.C. § 2284). The following highlights some of the new provisions in Title III.

Sec. 305. Transportation of Dangerous Materials and Terrorists.

This section makes it a federal crime to transport aboard a vessel an explosive, biological agent, chemical weapon, or radioactive or nuclear material with the intent that the material will be used to commit a federal crime of terrorism (as defined in 18 U.S.C. § 2332b(g)(5)(B)).

Procedural Changes: None at this time. If necessary, additional guidance may be issued in the future.

Sec. 309. Bribery Affecting Port Security.

This section makes it a federal crime to give or take a bribe with the intent to commit international or domestic terrorism affecting port security.

Procedural Changes: None at this time. If necessary, additional guidance may be issued in the future.

Sec. 311. Smuggling Goods from the United States.

This creates a new federal crime for illegally smuggling goods from the United States.

Procedural Changes: None at this time. If necessary, additional guidance may be issued in the future.

TITLE IV - COMBATING TERRORISM FINANCING ACT of 2005.

The U.S. Department of Justice indicated that this Title carries forward the overall strategy to stop terrorist-financing by making several adjustments to criminal statutes. It accomplishes this goal by enhancing penalties for terrorism financing and prohibiting terrorism financing through informal money networks, including hawalas. Illegal money laundering transmissions (18 U.S.C. § 1960) are now predicates for racketeering (RICO predicate list at 18 U.S.C. § 1961(1). Terrorism financing (18 U.S.C. § 2339C) and the receipt of foreign military

training (18 U.S.C. § 2339D) are now added to the money laundering predicate offense list (18 U.S.C. § 1956(c)(7)(D)). Finally, the Title authorizes the U.S. to confiscate the U.S. property related to certain acts of international terrorism against a foreign government or international organization (18 U.S.C. § 981(a)(1)(G)).

TITLE V - MISCELLANEOUS.

The Title creates a U.S. Department of Justice National Security Division which will be headed by a statutory Assistant Attorney General.

Sec. 506. Department of Justice Intelligence Matters.

This new section establishes a National Security Division (NSD) within the DOJ, headed by an Assistant Attorney General for National Security (AAGNS). This reorganization of DOJ is consistent with a recommendation by the WMD Commission that the "Department of Justice's primary national security elements - the Office of Intelligence Policy and Review, and the Counterterrorism and Counterespionage sections - should be placed under a new Assistant Attorney General for National Security."

> On March 2, 2006, the U.S. Department of Justice stated the following:
> This reorganization would bring together under one umbrella the attorneys from the Criminal Division's Counterterrorism and Counterespionage Sections and the attorneys from the Office of Intelligence Policy and Review (OIPR), with their specialized expertise in the Foreign Intelligence Surveillance Act and other intelligence matters. The new Assistant Attorney General will thus have all three core national security components under his or her control. He or she will lead a dedicated team acting in concert to accomplish their shared mission of protecting the national security while simultaneously safeguarding Americans' civil liberties. The Assistant Attorney General will also serve as the Department's primary liaison to the new Director of National Intelligence, and the new Division will gather expertise from across the Department to create a focal point for providing advice on the numerous legal and policy issues raised by the Department's national security missions.

Procedural Changes: The new Division will contain the Office of Intelligence Policy and Review, the Counterterrorism Section and the Counterespionage sections. The FBI's working relationships with these components will continue as normal. If the U.S. Department of Justice issues specific guidance at a future date, the guidance will be communicated to the FBI.

TITLE VI - SECRET SERVICE AUTHORIZATION AND TECHNICAL MODIFICATION ACT OF 2005.

The Title confirms that the Secret Service is a distinct entity within the U.S. Department of Homeland Security (DHS). Among several provisions, the Title establishes a "rolling" no trespass zone for individuals under Secret Service protection. It also prohibits fraud in connections with U.S. identification documents issued for a presidentially designated nationally significant event.

Procedural Changes Related to the Secret Service Act: None at this time. If necessary, additional guidance may be issued in the future.

To: All Divisions From: Office of the General Counsel
Re: 319X-HQ-A1487720-OGC, 04/07/2006

TITLE VII - COMBAT METHAMPHETAMINE EPIDEMIC ACT OF 2005.

Congress meant to provide a comprehensive approach toward controlling the methamphetamine problem. This Title increases the regulation of domestic and international commercial transactions in methamphetamine precursor chemical and enhances the criminal sanctions for methamphetamine related crimes, including the smuggling and selling of methamphetamine. For example, the Title requires sale of products containing ephedrine, pseudoephedrine, and phenylpropanolamine be limited to a 3.6 grams per customer per day, and the products be available only "behind the counter" at sales locations.

Procedural Changes Related to the Combat Methamphetamine Epidemic Act of 2005: None at this time. If necessary, additional guidance may be issued in the future.

Questions and Additional Information:

The National Security Law Branch (202-324-[redacted] is available to answer questions about this legislation. In addition, materials relating to the new legislation will be posted on the NSLB FBI Intranet website, which can be found through the FBI Office of General Counsel website.

b2

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

Read and Clear

♦♦

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

[DRAFTING DIVISION]
[STREET ADDRESS]
[CITY, STATE, ZIP CODE]
[MONTH, DAY, YEAR]

[MR./MRS./MS.] [Complete name]
[TITLE, IF AVAILABLE]
[NAME OF COMPANY]
[PHYSICAL STREET ADDRESS - NO P.O. BOX]
[CITY, STATE - NO ZIP CODE]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-07-2007 BY 65179 DMH/KSR/JW

1076786

Dear **[MR./MRS./MS.] [LAST NAME]:**

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (Section 201 of the Electronic Communications Privacy Act of 1986) (as amended), you are hereby directed to provide to the Federal Bureau of Investigation (FBI) the name, address, and length of service with respect to the following email/IP account(s):

[provide either or both - 1) person(s) to whom the email/IP address(es) is/was registered and/or 2)the email/IP address(es)

[NAME OF PERSON(S)]

[E-mail/IP ADDRESS(ES)]

[ON A SPECIFIC DATE]

or

[FOR THE PERIOD FROM [SPECIFIC DATE] TO [SPECIFIC DATE]
or [PRESENT]]

If the time period noted above is to the "present," that term is intended to direct production of information to the date of the processing of this letter. If providing information to the date of processing is not feasible, please provide information to the date of receipt of this letter.

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an

investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the constitution of the United States.

[Certification: The nondisclosure requirement is not an automatic feature of the NSL. If the supporting EC for this NSL included Option 1 (Invoking the Nondisclosure Requirement) then include the language in the following 3 paragraphs in the NSL.]

In accordance with 18 U.S.C. § 2709(c)(1), I certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person. Accordingly, 18 U.S.C. § 2709(c)(1) and (2) prohibits you, or any officer, employee, or agent of yours, from disclosing this letter, other than to those to whom disclosure is necessary to comply with the letter or to an attorney to obtain legal advice or legal assistance with respect to this letter.

In accordance with 18 U.S.C. § 2709(c)(3), you are directed to notify any persons to whom you have disclosed this letter that they are also subject to the nondisclosure requirement and are therefore also prohibited from disclosing the letter to anyone else.

In accordance with 18 U.S.C. § 2709(c)(4), if the FBI asks for the information, you should identify any person to whom such disclosure has been made or to whom such disclosure will be made. In no instance will you be required to identify any attorney to whom disclosure was made or will be made in order to obtain legal advice or legal assistance with respect to this letter.

[Include the following language in all NSLs.]

In accordance with 18 U.S.C. § 3511(a) and (b)(1), you have a right to challenge this letter if compliance would be unreasonable, oppressive, or otherwise unlawful, and you have the right to challenge the nondisclosure requirement set forth above.

In accordance with 18 U.S.C. § 3511(c), an unlawful failure to comply with this letter, including any nondisclosure requirement, may result in the United States bringing an enforcement action.

[MR./MRS./MS] [COMPLETE NAME]

You are directed to provide records responsive to this letter **[personally to a representative of the [DELIVERING DIVISION]** OR **through use of a delivery service to [OFFICE OF ORIGIN]** OR **through secure fax]** within [xxxx] business days of receipt of this letter.

Any questions you have regarding this letter should be directed only to the **[[DELIVERING DIVISION]** OR **[OFFICE OF ORIGIN],_depending on whether service is personal or through a delivery service]**. Due to security considerations, you should neither send the records through routine mail service nor non-secure fax, nor disclose the substance of this letter in any telephone conversation.

Your cooperation in this matter is greatly appreciated.

Sincerely yours,

[ADIC/SAC NAME]
[ASSISTANT DIRECTOR IN CHARGE/
SPECIAL AGENT IN CHARGE]

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date: 00/00/2007**

To: General Counsel **Attn:** Julie Thomas
Deputy General Counsel, NSLB

[COUNTERTERRORISM/ COUNTERINTELLIGENCE/CYBER] **Attn: [UNIT}**

[REQUESTING OFFICE] **Attn:** SSA [**SQUAD SUPERVISOR**]
SA [**CASE AGENT**]

[OFFICE OF ORIGIN] **Attn:** SA [**CASE AGENT**]
[SQUAD] [X]

[DELIVERING DIVISION] **Attn:** SSA [**SQUAD SUPERVISOR**]
(if using personal service) **[SQUAD] [X]**

From: [**DRAFTING DIVISION**]
[**APPROVING OFFICIAL**]
Contact: [**CASE AGENT, telephone number (000) 000-0000**)]

Approved By: [**ADIC NAME (IF APPLICABLE)**]
[**SAC NAME**]
[**ASAC NAME**]
[**CDC NAME**]
[**SSA NAME**]

DECLASSIFIED BY 65179 DMH/KSR/JW
ON 06-07-2007

1076786

Drafted By: [**LAST, FIRST, MIDDLE NAME: INITIALS**]

(U) **Case ID #:** ~~(S)~~ [**CASE FILE NUMBER**] (Pending)

(U) **Title:** ~~(S)~~ [**SUBJECT**]
[**AKA**] [**ALIAS (IF APPLICABLE)**]
[**IT/FCI - FOREIGN POWER**]
OO:[**OFFICE OF ORIGIN**]

Synopsis: (U) (NSLESI) Approves the issuance of an Electronic Communication Privacy Act(ECPA) National Security Letter (NSL)for email subscriber information; provides reporting data; and, if

(U)
To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**
Re: (S) **[CASE FILE NUMBER, 00/00/2007]**

necessary, transmits the NSL for delivery to the electronic communications service provider.

(U) (S) **Derived From: G-3**
Declassify On: [10-25 years based on information in the EC]

FULL/PRELIMINARY Investigation Instituted: (S) [00/00/2007]

(U) **Reference:** (S) **[CASE FILE NUMBER Serial XXX]**

Enclosures: (U) Enclosed for **[DELIVERING DIVISION or OFFICE OF ORIGIN, depending on whether service is personal or through a restricted delivery service or fax]** is an NSL dated **[00/00/2006]**, addressed to **[COMPANY POC NAME]**, **[TITLE (if available)]**, **[COMPANY NAME]**, **[COMPANY ADDRESS - NO P.O. BOX]**, **[CITY, STATE - NO ZIP CODE if using personal service]**, requesting the name, address, and length of service for the e-mail address holder(s) listed.

(U) **Details:** (S) A **[FULL/PRELIMINARY]** [**INTERNATIONAL/FOREIGN COUNTERINTELLIGENCE**] investigation of the subject, a **[USPER/NON-USPER]**, was authorized in accordance with the Attorney General Guidelines because **[Give a full explanation of the justification for opening and maintaining an investigation of the subject; barebones facts will not suffice and will cause the request to be rejected for lack of legal sufficiency]**. This electronic subscriber information is being requested to **[Fully state the relevance of the requested records to the investigation]**.

(U) This electronic communication documents the **[APPROVING OFFICIAL's]** approval and certification of the enclosed NSL. For mandatory reporting purposes, the enclosed NSL seeks subscriber information on **[NUMBER OF] [e-mail/IP address(es)]** from **[ISP #1]**; **[NUMBER OF] [e-mail/IP address(es)]** from **[ISP #2]**, etc.

(U) Arrangements should be made with the electronic communication service provider to provide the records **[personally to an employee of the DELIVERING division** OR **through use of a delivery service or secure fax to OFFICE OF ORIGIN]** within [**NUMBER OF**] business days of receipt of this request. The electronic communication service provider should neither send the

(U) To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**
Re: (~~S~~) **[CASE FILE NUMBER, 00/00/2007]**

records through routine mail service nor utilize the name of the subject of the request in any telephone calls to the FBI.

DISCLOSURE PROVISIONS

[Certification and Activation of the Nondisclosure Requirement: There is no longer an automatic prohibition that prevents the recipient of a National Security Letter from disclosing that the FBI has requested the information. To activate the nondisclosure requirement, the senior FBI official approving this EC must use Option 1 below and include in the EC (but not in the NSL) a brief statement of facts that justify the nondisclosure requirement. Option 2 is to be used in all cases where Option 1 is not used.]

[Option 1 - Invoking Nondisclosure Requirement]

(U) In accordance with 18 U.S.C. § 2709(c) I, the senior official approving this EC, certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person.

(U) (~~S~~) Brief statement of the facts justifying my certification in this case:

[Option 2 - Declining to invoke the nondisclosure requirement]

(U) I, the senior official approving this EC, have determined that the facts of this case do not warrant activation of the nondisclosure requirements under the applicable National Security Letter statute.

[Include the next 2 paragraphs in all ECs]

(U) Information received from an electronic communications service provider may be disseminated in accordance with the Attorney General Guidelines on National Security Investigations and Foreign Intelligence Collection and, with

(U)

To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**
Re: (~~S~~) **[CASE FILE NUMBER, 00/00/2007]**

respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(U) Any questions regarding the above can be directed to **[CASE AGENT, telephone number (000) 000-0000]**.

To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**

(U) Re: ~~(S)~~ **[CASE FILE NUMBER, 00/00/2007]**

LEAD (s):

Set Lead 1:

GENERAL COUNSEL

AT WASHINGTON, DC

(U) NSLB is requested to record the appropriate information needed to fulfill the Congressional reporting requirements for NSLs.

Set Lead 2: (Info)

[COUNTERTERRORISM/COUNTERINTELLIGENCE/CYBER]

AT WASHINGTON, DC

(U) At **[Unit]** Read and Clear

Set Lead 3:

[DELIVERING DIVISION - fif using personal service]

AT [CITY, STATE]

(U) Deliver the enclosed NSL as indicated above. Upon receipt of the information requested, **[DELIVERING DIVISION]** is requested to submit results to **[DRAFTING DIVISION]** and **[OFFICE OF ORIGIN, if applicable]**.

♦♦

[redacted]

b2

[redacted]

Model ECs and NSLs (as of 5/2/2007)

1. Telephone Subscriber EC (wpd)
2. Telephone Subscriber NSL (wpd)
3. Toll Record EC (wpd)
4. Toll Record NSL (wpd)
5. E-Mail Subscriber EC (wpd)
6. E-Mail Subscriber NSL (wpd)
7. Transactional Record EC (wpd)
8. Transactional Record NSL (wpd)
9. RFPA EC (wpd)
10. RFPA NSL (wpd)
11. 1681u(a) EC (wpd)
12. 1681u(a) NSL (wpd)
13. 1681u(b) EC (wpd)
14. 1681u(b) NSL (wpd)
15. 1681u(a) and (b) combination EC (wpd)
16. 1681u(a) and (b) combination NSL (wpd)
17. 1681v EC full credit report / IT investigation only (wpd)
18. 1681v NSL full credit report / IT investigation only (wpd)
19. NSL Delegation EC approved by Director (wpd)

Contacts

Contacts (all)

- Credit Bureaus
- Financial Institutions
- Internet Service Providers
- Telephone Companies
- Field Office POCs (doc)

Resources

Determining [redacted]

b2
b7E

Issue Spotting Checklist (doc)

1076786

NATIONAL SECURITY LETTERS (UPDATED 3/9/2007)

National Security letters are a specific type of investigative tool that allows the FBI to obtain certain limited types of information without court intervention:

1. Under the Electronic Communications Privacy Act, 18 U.S.C. §2709, the FBI can obtain telephone and email communication records from telephone companies and internet service providers.
2. Under the Right to Financial Privacy Act, 12 U.S.C.§3414(a)(5)(A), the FBI can obtain the records of financial institutions (which is very

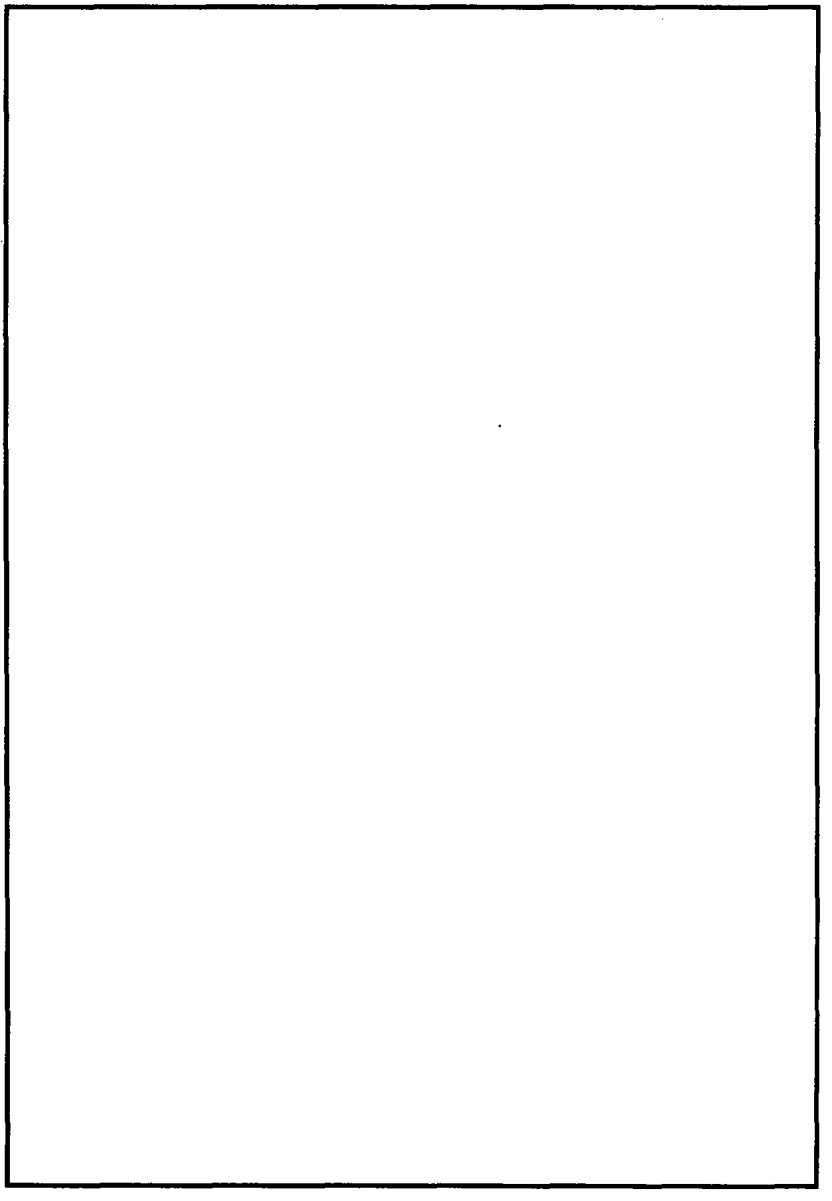
b2

[redacted]

broadly defined).

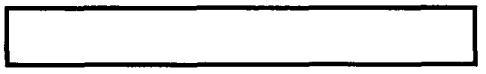
3. Under the Fair Credit Reporting Act, 15 U.S.C.§§1681u(a) and (b), the FBI can obtain a list of financial institutions and consumer identifying information from a credit reporting company.
4. Under the Fair Credit Reporting Act, 15 U.S.C. §1681v, the FBI can obtain a full credit report in an international terrorism case. This provision was created by the 2001 USA Patriot Act.

b5



The standard for issuing an NSL is relevance to an authorized investigation to protect against international terrorism or clandestine intelligence activities provided that such an investigation of a

b2



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 1681v NSL standard is slightly different to reflect that it applies only to international terrorism investigations.) Prior to the 2001 USA PATRIOT Act, the standard for issuance of an NSL was that the target or the communication was tied to a foreign power

b5

A request for an NSL has two parts. One is the NSL itself, and one is the EC approving issuance of the NSL. The authority to sign NSLs has been delegated to the Deputy Director, Executive Assistant Director and Assistant EAD for the National Security Branch; Assistant Directors and all DADs for CT/CI/Cyber; General Counsel; Deputy General Counsel for the National Security Law Branch; Assistant Directors in Charge in NY, D.C., and LA; and all SACs. The authority to certify and recertify the non-disclosure requirement of NSLs has also been delegated to those same persons. Persons acting in those capacities may not exercise such signature, certification or recertification authority.

THE NSL

All NSLs must be addressed to the specific company point of contact (many of which are listed on NSLB's website). All NSLs should identify the statutory authority for the request, the type of records requested, and provide identifying information to assist the company in processing the request. One change has been made to the opening paragraph; recipients are now "DIRECTED" to produce the information rather than simply "requested."

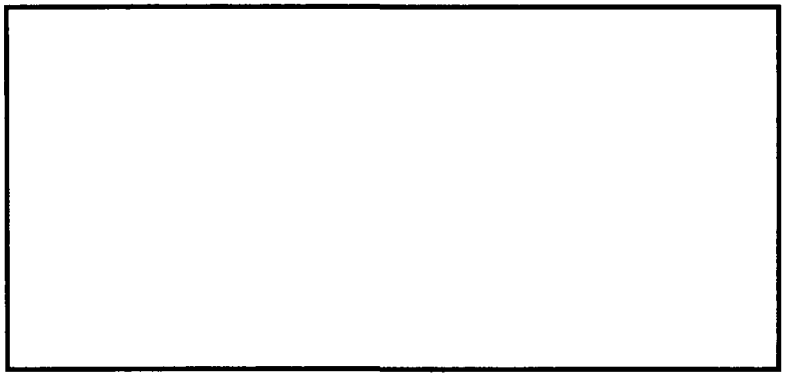
All NSLs require a certification that the records

b2

sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities and that an investigation of a USP is not conducted solely on the basis of First Amendment rights (with the 1681v NSL certification being slightly different to reflect its application only to international terrorism investigations).

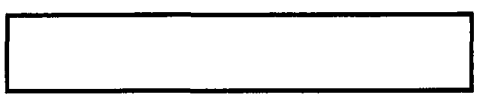
The major recent change in the format of the NSL derives from the newly enacted USA PATRIOT Improvement and Reauthorization Act of 2005 (2005 USA PATRIOT Act). The non-disclosure provision is no longer automatically included in the NSL. If the requesting party seeks to have a non-disclosure provision included in the NSL, there needs to be a certification in the NSL that the disclosure may endanger national security, interfere with a criminal, counter terrorism, or counterintelligence investigation, or interfere with diplomatic relations or endanger a life. Once the certification is made, the recipient is under an obligation not to disclose the fact of the request to anyone except those in the company that have a need to know and to legal counsel, if necessary. Further, as to those NSL which contain a non-disclosure provision, the NSL recipient is informed that he must convey the non-disclosure requirement to persons who have such a need to know, and that, if asked, he must inform the FBI of the names of those persons. In addition, the NSL recipient is informed that he may challenge that non-disclosure provision. In all NSLs, the recipient is informed of his right to challenge the NSL itself if compliance would be unreasonable, oppressive or otherwise unlawful, as well as the right of the FBI to enforce the NSL, including the non-disclosure provision, if there is one. The recipient is also informed that he may return the information to the FBI via federal express, secure fax, or personal delivery but not via regular mail or non-secure fax.

b5



NEW LANGUAGE OF THE MODEL NSLS

b2



The following is the new language that you will now see in model NSLs. The first three paragraphs are optional, to be used if there is a need for non-disclosure.

In accordance with [cite to pertinent statute], I certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counter terrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person. Accordingly, 18 U.S.C. § 2709(c)(1) and (2) prohibits you, or any officer, employee, or agent of yours, from disclosing this letter, other than to those to whom disclosure is necessary to comply with the letter or to an attorney to obtain legal advice or legal assistance with respect to this letter.

In accordance with [cite to pertinent statute], you are directed to notify any persons to whom you have disclosed this letter that they are also subject to the nondisclosure requirement and are therefore also prohibited from disclosing the letter to anyone else.

In accordance with [cite to pertinent statute], if the FBI asks for the information, you should identify any person to whom such disclosure has been made or to whom such disclosure will be made. In no instance will you be required to identify any attorney to whom disclosure was made or will be made in order to obtain legal advice or legal assistance with respect to this request.

In accordance with [cite to pertinent statute], you have a right to challenge this request if compliance would be unreasonable, oppressive, or otherwise unlawful and the right to challenge the nondisclosure requirement set forth above.

In accordance with [cite to pertinent

statute], an unlawful failure to comply with this letter, including any nondisclosure requirement, may result in the United States bringing an enforcement action.

COVER EC

The cover EC serves five functions.

1. It documents the predication for the NSL by stating why the information sought is relevant to an authorized investigation,
2. It documents the approval of the NSL by appropriate personnel,
3. It documents certification of the necessity for non-disclosure, when applicable,
4. It contains information needed to fulfill Congressional reporting requirements for each type of NSL (subject's USP status, type of NSL issued, and the number of phone numbers, email addresses, account numbers or individual records being requested in the NSL), and
5. It transmits the NSL to NSLB for reporting requirements, to CTD, CD, or Cyber for informational purposes, and, in the case of personal service, to the requesting squad or delivering field division for delivery.

The EC must reference an investigative case file, and not a control file, to which the information sought is relevant. See EC dated 2/23/2007, Guidance on the Reference of Investigative Case File Number in NSL-authorizing EC, 319X-HQ-A1487720-OGC, serial 326. The EC does not need to reference an NSLB file any longer. However, there must be a lead to NSLB, for informational and reporting purposes, and a lead to the relevant HQ operational unit, (CTD, CD, Cyber), for informational purposes. There does not need to be a hard copy of the EC or NSL sent to NSLB or the relevant HQ operational unit.

The requirement for certification for the need for a non-disclosure provision is the major change in the format of the EC. It derives from the USA PATRIOT Improvement and Reauthorization Act of 2005 in that the requesting party must affirmatively take steps to have a non-disclosure provision included in the NSL; it is not automatic anymore. If a non-disclosure provision is sought, the EC must set forth a factual predicate to require such a provision.

As a general matter, the certification must assert that disclosure may endanger national security, interfere with a criminal, counter terrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person. More specifically, the manner in which those dangers may arise from disclosure of the issuance of an NSL could include:

1.

2.

b5

b2
b7E

3.

4.

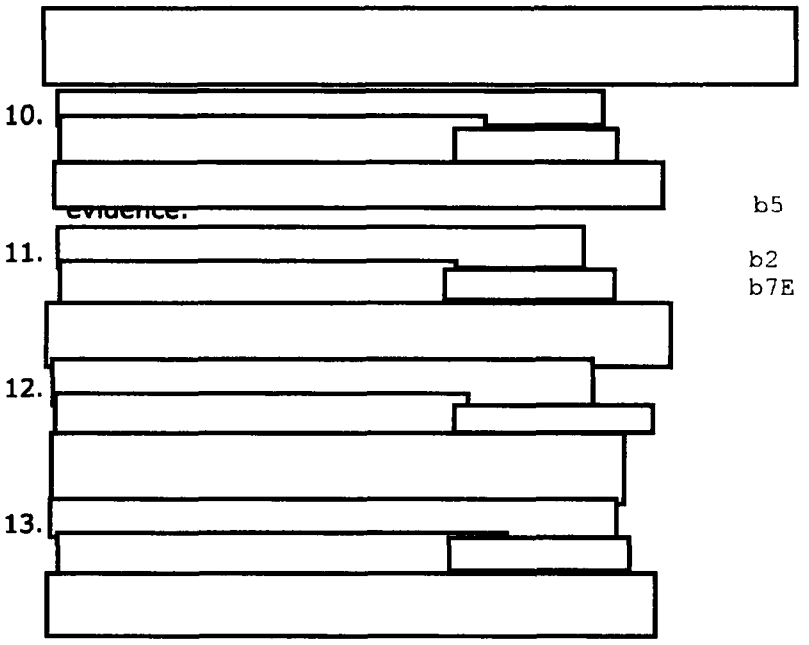
5.

6.

7.

8.

9.



b5

b2
b7E

This is not an exclusive list. Therefore, if there are other reasons for requesting a non-disclosure provision, those reasons should be set forth in the EC.

NEW LANGUAGE OF THE MODEL ECS

The following is the new language that you will now see in model ECs.

[Option 1 - Invoking Nondisclosure Requirement]

> *(U) In accordance with [cite to pertinent statute] I, the senior official approving this EC, certify that a disclosure of the fact that the FBI has sought or obtained access to the information sought by this letter may endanger the national security of the United States, interfere with a criminal, counter terrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person.*
>
> *(S) Brief statement of the facts justifying my certification in this case:*

[Option 2 - Declining to invoke the nondisclosure requirement]

> *(U) I, the senior official approving this*

b2

EC, have determined that the facts of this case do not warrant activation of the nondisclosure requirements under the applicable National Security Letter statute.

VARIOUS GUIDANCES

Attached are guidances that relates to NSLs.

1. EC dated 5/27/2005, 319X-HQ-A1487720-OGC, serial 20, which authorizes the use of return dates.
2. EC dated 6/29/2005, 319X-HQ-A1487720-OGC, serial 24, which relates to use of restricted delivery services to serve NSLs.
3. EC dated 3/20/2006, 319X-HQ-A1487720-OGC, serial 213, which permits the FBI to serve NSLs by non-secure fax under certain conditions.
4. EC dated 4/11/2006, 319X-HQ-A1487720-OGC, serial 222, which relates to the FBI's reimbursement policy for NSLs.
5. EC dated 3/09/2006, 319X-HQ-A1487720-OGC, serial 210, which delegated NSL approval and certification authority.
6. EC dated 3/09/2007, 319X-HQ-A1487699-RMD, serial 17, which created the NSL "document type" in ACS.
7. NSL powerpoint, which include a summary of NSL information.
8. EC dated 4/4/2007, 319X-HQ-A1487720-OGC, Procedures for Redacting NSL Results

The relevant delegation of signature authority EC is the one issued on 3/09/2006, set forth above. This encompasses all signature delegations and takes precedent over all of the other delegations (and supercedes some). So please look to it to determine who has authority to sign NSLs. The EC dated 3/09/2006 also provides for delegation of the authority to certify that the non-disclosure provision is necessary with respect to a given NSL. Further, this delegation also provides authority with respect to the ability to recertify the need for non-disclosure were the non-disclosure to be challenged a year or more after service of the NSL. As has been DOJ policy for quite some time, a person in an acting position does not have the authority to sign NSLs. It follows that those in an acting position do not have authority to certify or recertify the non-disclosure provision, either. Although the

b2

[redacted]

3/09/2006 delegation contains all the relevant NSL delegations, it is not referenced in the model EC. This is a change from the previous model ECs.

If you need to view the statutory authority for these NSLs, copies of the ECPA, RFPA, and FCRA statutes can be found on the OGC main library website. In addition, the 2001 and 2005 Patriot Acts are also on the OGC main library website.

APPROVAL STANDARD FOR NSLS

NSLs are reviewed by CDCs at the field office level. At headquarters, they are reviewed by NSLB. At all levels, they must meet the legal standards set forth above, namely relevance to an authorized national security investigation. [redacted] Otherwise, any target with a telephone or a bank account is subject to an NSL. And that is not the standard for issuance of an NSL. The model EC now states that a full recitation of the reason for initiating and maintaining the investigation is necessary in order to justify an NSL. The reason is common sensical - there can be no reason to issue an NSL if the subject matter or issue to which it supposedly relates is not worthy of investigation or if the investigation is based solely on the exercise of First Amendment rights. [redacted] In other words, in order for an NSL to meet the legal standard set forth in the statutes, the reviewing party has to assure that there is a proper reason for investigating the target and not an improper reason, for instance, exercising First Amendment rights..

b2
b7E
b5

Moreover, the legal review that is done by the CDCs is consistent with the factual review that should be done by SACs in certifying that the NSL is relevant to an authorized national security investigation and that the investigation is not based on the exercise of First Amendment rights by a U.S.P. An SAC can no more make the required certification than the CDC can make the required legal review if presented only with barebones information of the existence of an investigation and a target's telephone or bank account. Thus, the recitation of facts about the reason for initiating and maintaining an investigation serves to support

[redacted] b2

both the SAC certification and the CDC legal review.

Thus, approval of an NSL needs to include a review of why the FBI is conducting the investigation. The fact that there is no legal review of the opening of an investigation does not preclude review of the reason for the investigation in the course of determining whether an NSL request meets the legal standard of the NSL statute.

NO EXIGENT LETTERS

The practice of using exigent letters to obtain NSL-type information prior to issuance of an NSL has been prohibited. See EC dated 3/1/2007, Telephone Inquiries; Emergency Disclosure Provision, 319X-HQ-A1487720-OGC, Serial 331. Instead, in emergency circumstances, a letter under 18 U.S.C. 2702 (which letters are also sometimes called "exigent letters" by the field but they differ from those that have been used at HQ because they do in fact reference 2702 and thus are acceptable) may be issued. The letter, a sample of which is attached to the above-referenced EC, describes the circumstances of the emergency and requests that the recipient make a determination that in fact "an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information." 18 U.S.C. § 2702(b)(8) and (c)(4). Both content and customer records are available under this statute. The disclosure does not need to be followed by legal process, although some recipients may require such process, and a promise in advance, in order to release the records.

REPORTING REQUIREMENTS

NSLB is required to report information about its NSL usage to Congress. Therefore, it is crucial that the portion of the EC that addresses reporting requirements is accurately addressed. While an EC may cover more than one target, more than one account, and more than one recipient, when all of the requests are related, the EC must break down the number of targeted phone numbers/email accounts/financial accounts that are addressed to each and every NSL recipient. Therefore, if there are three targets, ten accounts, and six recipients of an NSL, then the EC must state how many accounts are the subject of the NSL to recipient 1, to recipient 2, etc. It is not sufficient to tell NSLB that there are ten accounts and six recipients.

In addition, under the 2005 USA PATRIOT ACT, we must now report the USP status of the subject of the NSL request (as opposed to the target of the investigation to which the NSL is relevant). While the subject is often the target of the investigation, that may not always be the case. So the EC must reflect the USP status is of the subject of the request - the person whose information we are obtaining. If we are obtaining information about more than one person, the EC must reflect the USP status of each of those persons. (See the form ECs, which make clear that the USP status applies to the subject(s) of the request for information.)

Also, to make sure that NSLB is reporting the correct type of information that is being sought, please be sure that the EC is consistent as to the type of information that is being sought. Keep in mind that when asking for toll billing records or for transactional records, the information produced will include subscriber information. Thus, in that case, the EC need only state the request is for toll billing records or transactional records, and the reporting paragraph should be consistent and state that toll billing or transactional records are being sought for x number of accounts, and, if multiple recipients, from each of recipients #1, #2, etc.

DISSEMINATION OF NSL MATERIAL

Information obtained through the use of an NSL may be disseminated in accordance with general standards set forth in The Attorney General's Guidelines for FBI National Security Investigation and Foreign Intelligence Collection (NSIG). Dissemination is further subject to specific statutory limitations (e.g., toll record NSL statute, ECPA, 18 U.S.C. §2709, and financial record NSL statute, RFPA, 12 U.S.C. §3414(a)(5)(B), permit dissemination if per NSIG and information is clearly relevant to responsibilities of recipient agency; limited credit information NSL statute, FCRA, 15 U.S.C. §1681u, permits dissemination to other federal agencies as may be necessary for the approval or conduct of an FCI investigation; no special statutory rules for dissemination under full credit report NSL statute, FCRA, 15 U.S.C. §1681v).

Although the requesting EC is generally classified because it provides reasons for the investigation and the need for the NSL, the NSLs themselves are not classified, nor is the material received in return from NSLs classified. That information may be used in criminal proceedings without any declassification

issue. [redacted]

[redacted]

b2
b7E
b5

POCS FOR NSL RECIPIENTS

Attached also please find a list of the names and addresses of appropriate offices/persons to whom NSLs should be addressed [redacted]

b2

[redacted]

Since OGC generally does not have contact with these entities, we rely on the field to let us know when these points of contact are outdated or when new entities come into play for which POCs would be useful . So please let us know when you run across POC information that headquarters and other field offices might find useful.

FINANCIAL INSTITUTION NSLS

[redacted]

b2
b7E
b5

[redacted]

b2

Until such time as the standard RFPA NSL has been amended to reflect the above, if you run into this problem with a financial institution, please contact your CDC or NSLB.

MISCELLANEOUS

If you come across useful information on other NSL-related topics, please email or call [redacted] of NSLB (202-324[redacted] and we will add it to this website. Further, if there are modifications or additions to our Point of Contact listings, please notify [redacted] of NSLB.

b6
b7C
b2

Last modified at 05/03/2007 06:54 AM

USER TIPS **LEGAL NOTICE**