Freedom of Information and Privacy Acts

SUBJECT: NATIONAL SECURITY LETTERS
FOLDER: CTD - SECTION 1

Federal Bureau of Investigation

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ COVER SHEET 05/03/2007

Total Deleted Page(s) ~ 48
Page 32 ~ b2, b7E
Page 33 ~ b2, b7E
Page 39 ~ b2, b4, b6, b7C, b7D, b7E
Page 40 ~ b2, b4, b6, b7C, b7D, b7E
Page 41 ~ b2, b4, b6, b7C, b7D, b7E
Page 42 ~ b2, b4, b6, b7C, b7D, b7E
Page 43 ~ b2, b4, b6, b7C, b7D, b7E
Page 44 ~ b2, b4, b6, b7C, b7D, b7E
Page 45 ~ b2, b4, b6, b7C, b7D, b7E
Page 46 ~ b2, b4, b6, b7C, b7D, b7E
Page 47 ~ b2, b4, b6, b7C, b7D, b7E
Page 48 ~ b2, b4, b6, b7C, b7D, b7E
Page 49 ~ b2, b4, b6, b7C, b7D, b7E
Page 50 ~ b2, b4, b6, b7C, b7D, b7E
Page 51 ~ b2, b4, b6, b7C, b7D, b7E
Page 52 ~ b2, b4, b6, b7C, b7D, b7E
Page 53 ~ b2, b4, b6, b7C, b7D, b7E
Page 54 ~ b2, b4, b6, b7C, b7D, b7E
Page 55 ~ b2, b4, b6, b7C, b7D, b7E
Page 56 ~ b2, b4, b6, b7C, b7D, b7E
Page 57 ~ b2, b4, b6, b7C, b7D, b7E
Page 58 ~ b2, b4, b6, b7C, b7D, b7E
Page 59 ~ b2, b4, b6, b7C, b7D, b7E
Page 60 ~ b2, b4, b6, b7C, b7D, b7E
Page 61 ~ b2, b4, b6, b7C, b7D, b7E
Page 62 ~ b2, b4, b6, b7C, b7D, b7E
Page 63 ~ b2, b4, b6, b7C, b7D, b7E
Page 64 ~ b2, b4, b6, b7C, b7D, b7E
Page 65 ~ b2, b4, b6, b7C, b7D, b7E
Page 66 ~ b2, b4, b6, b7C, b7D, b7E
Page 67 ~ b2, b4, b6, b7C, b7D, b7E
Page 68 ~ b2, b4, b6, b7C, b7D, b7E
Page 69 ~ b2, b4, b6, b7C, b7D, b7E
Page 70 ~ b2, b4, b6, b7C, b7D, b7E
Page 71 ~ b2, b4, b6, b7C, b7D, b7E
Page 72 ~ b2, b4, b6, b7C, b7D, b7E
Page 73 ~ b2, b4, b6, b7C, b7D, b7E
Page 74 ~ b2, b4, b6, b7C, b7D, b7E
Page 75 ~ b2, b4, b6, b7C, b7D, b7E
Page 76 ~ b2, b4, b6, b7C, b7D, b7E
Page 77 ~ b2, b4, b6, b7C, b7D, b7E
Page 78 ~ b2, b4, b6, b7C, b7D, b7E
Page 79 ~ b2, b4, b6, b7C, b7D, b7E
Page 80 ~ b2, b4, b6, b7C, b7D, b7E

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

Page 81 ~ b2, b4, b6, b7C, b7D, b7E
Page 82 ~ b2, b4, b6, b7C, b7D, b7E
Page 83 ~ b2, b4, b6, b7C, b7D, b7E
Page 84 ~ b2, b4, b6, b7C, b7D, b7E

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

(Rev. 03-09-2006)

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

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 00/00/2006

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]**
[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]

(U)

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

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

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

Synopsis: (U) Approves the issuance of an FCRA Section 1681u(a) National Security Letter (NSL) for financial institution listings; provides reporting data; and transmits the NSL for delivery to the consumer reporting agency.

(U) ~~(S)~~ **Derived From: G-3**

~~SECRET~~

To: [DELIVERING DIVISION] From: [DRAFTING DIVISION]
(U) Re: ~~(S)~~ [CASE FILE NUMBER, 00/00/2005]

Declassify On: [10 Years from Date of EC]

(U) FULL/PRELIMINARY Investigation Instituted: 00/00/2005

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

Enclosure(s): (U) Enclosed for [DELIVERING DIVISION] 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 and addresses of financial institutions at which the listed consumer maintains or has maintained an account.

(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]. This financial institution 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 the financial institution listings for [NUMBER OF] individual(s) from [CONSUMER REPORTING AGENCY A]; [NUMBER OF] individual(s) from [CONSUMER REPORTING AGENCY B], etc. [If you know how many credit report consumers are USPs, please state.]

(U) The enclosed NSL will be personally delivered by [DELIVERING DIVISION].

(U) Arrangements should be made with the consumer reporting agency to provide the records [personally to an employee of the DELIVERING DIVISION] within [NUMBER OF] business days of receipt of this request. The consumer reporting agency should neither send the records through routine mail delivery nor utilize the name of the subject of the request in any telephone calls to the FBI.

(U) Information received from a consumer reporting agency may not be disseminated outside the FBI, except to other Federal agencies in accordance with the Attorney General Guidelines for FBI National Security Investigations and Foreign Intelligence Collection and only as may be necessary for the

(U) To: [DELIVERING DIVISION] From: [DRAFTING DIVISION]
(U) Re: (S) [CASE FILE NUMBER, 00/00/2005]

conduct of a foreign counterintelligence investigation, or where the information concerns a person subject to the Uniform Code of Military Justice, to appropriate authorities within the military department concerned as may be necessary for the conduct of a joint foreign counterintelligence investigation.

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

NONDISCLOSURE PROVISION [NEW REQUIREMENT]

[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 15 U.S.C. § 1681u(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:

OR

[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.

To: [DELIVERING DIVISION] From: [DRAFTING DIVISION]
Re: (~~S~~) [CASE FILE NUMBER, 00/00/2005]

(U)

To: **[DELIVERING DIVISION]** **From: [DRAFTING DIVISION]**
(U) Re: (~~S~~) **[CASE FILE NUMBER, 00/00/2005]**

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 OFFICE]

[AT CITY, STATE]

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

♦♦

[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]

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

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 15, United States Code (U.S.C.), Section 1681u(a) (the Fair Credit Reporting Act, as amended), you are hereby directed to provide the Federal Bureau of Investigation (FBI) the names and addresses of all financial institutions (as defined in Title 12, U.S.C., Section 3401) at which the below-named consumer(s) maintains or has maintained an account:

NAME(S):

ADDRESS(ES): [if available]

DATE(S) OF BIRTH: [if available]

SOCIAL SECURITY NUMBER(S): [if available]

In accordance with Title 15, U.S.C., Section 1681u(a), I certify that such information is sought for the conduct of an authorized investigation to protect against 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.

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

[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 15 U.S.C. § 1681u(d)(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, 15 U.S.C. § 1681u(d)(1) and (3) 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 15 U.S.C. § 1681u(d)(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 15 U.S.C. § 1681u(d)(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 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]

(Rev. 03-09-2006)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 00/00/2006

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]**
[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

(U) **Drafted By:** **[LAST FIRST MIDDLE NAME: INITIALS]**

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

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

Synopsis: (U) Approves the issuance of an FCRA Section 1681u(b) National Security Letter (NSL) for consumer identifying information; provides reporting data; and transmits the NSL for delivery to the consumer reporting agency.

(U) ~~(S)~~ **Derived From : ~~G-3~~**
Declassify On: ~~[10 Years from Date of EC]~~

~~SECRET~~

To: [DELIVERING DIVISION] From: [DRAFTING DIVISION]
(U) Re: (S) [CASE FILE NUMBER, 00/00/2005]

(U) **FULL/PRELIMINARY Investigation Instituted: 00/00/2005**

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

Enclosure(s): (U) Enclosed for **[DELIVERING DIVISION** 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 consumer identifying information relating to the consumer 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]**. This consumer identifying 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 consumer identifying information for **[NUMBER OF]** individual(s)from **[CONSUMER REPORTING AGENCY A]**; **[NUMBER OF]** individual(s) from **[CONSUMER REPORTING AGENCY B]**; etc. **[If you know how many credit report consumers are USPs, please state.]**

(U) The enclosed NSL will be personally delivered by **[DELIVERING DIVISION]**.

(U) Arrangements should be made with the consumer reporting agency to provide the records **[personally to an employee of the DELIVERING DIVISION]** within **[NUMBER OF]** business days of receipt of this request. The consumer reporting agency 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.

(U) Information received from a consumer reporting agency may not be disseminated outside the FBI, except to other Federal agencies in accordance with the Attorney General Guidelines for FBI National Security Investigations and Foreign Intelligence Collection and only as may be necessary for the conduct of a foreign counterintelligence investigation, or where the information concerns a person subject to the Uniform Code of

To: [DELIVERING DIVISION] From: [DRAFTING DIVISION]
(U) Re: (S) [CASE FILE NUMBER, 00/00/2005]

Military Justice, to appropriate authorities within the military department concerned as may be necessary for the conduct of a joint foreign counterintelligence investigation

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

NONDISCLOSURE PROVISION [NEW REQUIREMENT]

[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 15 U.S.C. § 1681u(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:

OR

[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.

To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**
Re: (U) **[CASE FILE NUMBER, 00/00/2005]**

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 OFFICE]

[AT CITY, STATE]

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

♦♦

[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]

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

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 15, United States Code (U.S.C.), Section 1681u(b) (the Fair Credit Reporting Act, as amended), you are hereby directed to provide the Federal Bureau of Investigation (FBI) the names, address, former addresses, places of employment, or former places of employment of the below-named consumer(s):

NAME(S):

ADDRESS(ES): [if available]

DATE(S) OF BIRTH: [if available]

SOCIAL SECURITY NUMBER(S): [if available]

In accordance with Title 15, U.S.C., Section 1681u(a), I certify that such information is sought for the conduct of an authorized investigation to protect against 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.

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

[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 15 U.S.C. § 1681u(d)(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, 15 U.S.C. § 1681u(d)(1) and (3) 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 15 U.S.C. § 1681u(d)(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 15 U.S.C. § 1681u(d)(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 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]

(Rev. 03-09-2006)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 00/00/2006

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

[COUNTERTERRORISM] **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]**
[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 06-08-2007

(U) **Drafted By:** **[LAST FIRST MIDDLE NAME: INITIALS]**

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

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

Synopsis: (U) Approves the issuance of an FCRA Section 1681v National Security Letter (NSL) for a full credit report in an international terrorism investigation; provides reporting data; and transmits the NSL for delivery to the consumer reporting agency.

(U) ~~(S)~~ **Derived ~~From~~ : G-3**

~~SECRET~~

~~SECRET~~

(U) To: [DELIVERING DIVISION] From: [DRAFTING DIVISION]
Re: (S) [CASE FILE NUMBER, 00/00/2005]

Declassify On: [10 Years from Date of EC]

(U) FULL/PRELIMINARY Investigation Instituted: 00/00/2005

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

Enclosure(s): (U) Enclosed for **[DELIVERING DIVISION]** 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 a full consumer credit report and all information in its files relating to the consumer listed.

(U) **Details:** (S) A **[FULL/PRELIMINARY]** 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]**. This full credit report 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 reporting purposes, the enclosed NSL seeks **[NUMBER OF]** of credit reports from **[CONSUMER REPORTING AGENCY A]**, **[NUMBER OF]** credit reports from **[CONSUMER REPORTING AGENCY B]**, etc. **[If you know how many credit report consumers are USPs, please state.]**

(u) The enclosed NSL will be delivered personally by **[DELIVERING DIVISION]**.

(U) Arrangements should be made with the consumer reporting agency to provide the records **[personally to an employee of the DELIVERING DIVISION]** within **[NUMBER OF]** business days of receipt of this request. The consumer reporting agency should neither send the records through routine mail delivery nor utilize the name of the subject of the request in any telephone calls to the FBI.

(U) Information received from a consumer reporting agency may be disseminated to an agency of the United States Government in accordance with the Attorney General Guidelines for FBI National Security Investigations and Foreign Intelligence Collection.

(U) To: **[DELIVERING DIVISION]** From: **[DRAFTING DIVISION]**
Re: ~~(S)~~ **[CASE FILE NUMBER, 00/00/2005]**

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

NONDISCLOSURE PROVISION [NEW REQUIREMENT]

[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 15 U.S.C. § 1681v 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:

OR

[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, 00/00/2005]**

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

AT WASHINGTON, DC

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

Set Lead 3: (Action)

[DELIVERING OFFICE]

[AT CITY, STATE]

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

♦♦

[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]

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

Pursuant to Executive Order 12333, dated December 4, 1981, and 15 U.S.C. § 1681v of the Fair Credit Reporting Act (as amended), you are hereby directed to provide the Federal Bureau of Investigation (FBI) with a copy of a consumer credit report and all other information contained in your files for the below-listed consumer(s):

NAME(S):

ADDRESS(ES): **[if available]**

DATE(S) OF BIRTH: **[if available]**

SOCIAL SECURITY NUMBER(S): **[if available]**

In accordance with Title 15, U.S.C. § 1681v, I certify that the information sought is necessary to conduct an authorized investigation of, or intelligence or counterintelligence activities or analysis related to, international terrorism.

[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 15 U.S.C. § 1681v(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, 15 U.S.C. § 1681v(1) and (3) 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 15 U.S.C. § 1681v(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 15 U.S.C. § 1681v(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 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.

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.

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

Your cooperation in this matter is appreciated.

Sincerely,

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

(Rev. 03-09-2006)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 00/00/2006

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 06-08-2007

(U) **Drafted By:** **[LAST, FIRST MIDDLE: INITIALS]**

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

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

(U) **Synopsis:** ~~(S)~~ Approves the issuance of an 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 years from date of EC]"**~~

~~SECRET~~

(U) To: [CTD/CD] From: [DRAFTING DIVISION]
Re: (S) [CASE FILE NUMBER, 00/00/2005]

FULL/PRELIMINARY Investigation Instituted: (S) **00/00/2005**

(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 **[00/00/2005]**, 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).

(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 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.

[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 12 U.S.C. § 3414(a) I, the senior official approving this EC, certify that a disclosure of the fact that

(U) To: [CTD/CD] From: [DRAFTING DIVISION]
Re: (~~S~~) [CASE FILE NUMBER, 00/00/2005]

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 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].**
LEAD(s):

To: **[CTD/CD]** From: **[DRAFTING DIVISION]**
(U) Re: ~~(S)~~ **[CASE FILE NUMBER, 00/00/2005]**

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]**.

♦♦

[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]

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 request for the types of information that your financial institution might consider to be a financial record.

In accordance with Title 12, U.S.C. Section 3414(a)(5)(A), I certify that the requested 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 request.

[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 request 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

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

requirement, may result in the United States bringing an enforcement action.

You are requested to provide records responsive to this request **[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 request.

Any questions you have regarding this request 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 request 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. 01-31-2003)

~~SECRET/ORCON/NOFORN~~//FISA

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 09/27/2006

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

From: Counterterrorism
CXS/ECAU/Room 4343
Contact: IA Best D. Analyst, 202/your phone

Approved By: Billy Joseph Jr
Frahm Charles E
Love Jennifer Smith
Wall Thomas S
Sheldon Kristen L
Your SSA

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE
DATE: 06-08-2007
CLASSIFIED BY 65179 DMH/KSR/JW
REASON: 1.4 (C)
DECLASSIFY ON: 06-08-2032

Drafted By: Analyst Best D:bda

(U) b1 **Case ID #:** (S) [redacted] (Pending)
~~(S)~~ File number which is a PI or FF (Pending)

(U) **Title:** ~~(S)~~ ELECTRONIC COMMUNICATIONS ANALYSIS
NATIONAL SECURITY/PATRIOT ACT LETTER MATTERS

(U) ~~(S)~~ Title of file number which is a PI or FF

Synopsis: (U) Requests the issuance of an Electronic Communications Privacy Act ("ECPA") National Security Letter (NSL) for subscriber and transactional records information.

(U) ~~(S)~~ **Derived ~~From~~ : G-3**
Declassify On: X1

(U) Full Investigation Initiated: XX/XX/200X
or
(U) Preliminary Investigation Initiated: XX/XX/200X, set to expire XX/XX/200X.

Administrative: (S) This document is classified SECRET/ORCON/NOFORN//FISA. Portions of this document carrying classification markings may not be incorporated into any criminal affidavit, criminal court proceeding or unclassified

To: General Counsel From: Counterterrorism
Re: (S) [redacted] 09/27/2006 b1

investigative file. The information in this document is intended to be used for lead or background purposes only.

[redacted] b2 b7E

(U) (S) [redacted] b2 b7E

(U) (S) [redacted] b1

Details: (U) (S) A **[FULL/PRELIMINARY]** **[INTERNATIONAL/FOREIGN COUNTERINTELLIGENCE]** investigation of XX, the subject of the captioned case, 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]**.

(U) (S) Articulate the connection between the email address you are requesting an NSL upon and the subject listed above.

(U) (S) ECAU requests a NSL be issued to for the email address XXXX in order to **[Fully state the relevance of the requested records to the investigation]**. This email address was verified and preserved on XX/XX/200X.

(U) (S) It is requested that NSLB issue a NSL to XXX for subscriber and transactional records pertaining to the email address XXXX.com.

To: General Counsel From: Counterterrorism
Re: (S) [redacted] 09/27/2006

b1

(U) (S) It is further requested that NSLB ensure the records obtained from XXX are submitted to FBIHQ, CTD/CXS/ECAU, Room 4343, IA Best D. Analyst.

To: General Counsel From: Counterterrorism
Re: (S) [redacted] 09/27/2006 b1

LEAD(s):

Set Lead 1: (Action)

GENERAL COUNSEL

AT WASHINGTON, DC

(U) (S) This electronic communication requests NSLB prepare a National Security Letter (NSL) to obtain subscriber and transactional records associated with the email address XX, which was verified and preserved on XX/XX/2006. The NSL should be directed to XX (name of the ISP) at address of ISP. Results of the NSL should be submitted to FBIHQ, CTD/CXS/ECAU, Room 4343, IA Best D. Analyst.

♦♦

SECRET

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

October 20, 2006

(S)

[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 06-07-2007
CLASSIFIED BY 65179 DMH/KSR/JW
REASON: 1.4 (C)
DECLASSIFY ON: 06-07-2032

b1
b6
b7C
b7D

Re: [redacted]

(S)

[redacted]

Sincerely,

b6
b7C

[redacted]
Unit Chief
Communications Analysis Unit

By:

Supervisory Special Agent

SECRET

Freedom of Information and Privacy Acts

SUBJECT: NATIONAL SECURITY LETTERS
FOLDER: CTD| CD| Volume 1

Federal Bureau of Investigation

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ COVER SHEET

Total Deleted Page(s) ~ 16
Page 22 ~ b2, b7E
Page 23 ~ Duplicate Court document /CC:Docket # 96-115
Page 24 ~ Duplicate
Page 25 ~ Duplicate
Page 26 ~ Duplicate
Page 27 ~ Duplicate
Page 28 ~ Duplicate
Page 29 ~ Duplicate
Page 30 ~ Duplicate
Page 31 ~ Duplicate
Page 32 ~ Duplicate
Page 33 ~ Duplicate
Page 34 ~ Duplicate
Page 35 ~ Duplicate
Page 36 ~ Duplicate
Page 37 ~ Duplicate

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

[Code of Federal Regulations]
[Title 47, Volume 3]
[Revised as of October 1, 2005]
From the U.S. Government Printing Office via GPO Access
[CITE: 47CFR42.6]

[Page 6]

TITLE 47--TELECOMMUNICATION

CHAPTER I--FEDERAL COMMUNICATIONS COMMISSION (CONTINUED)

PART 42_PRESERVATION OF RECORDS OF COMMUNICATION COMMON CARRIERS--Table
of Contents

Sec. 42.6 Retention of telephone toll records.

Each carrier that offers or bills toll telephone service shall retain for a period of 18 months such records as are necessary to provide the following billing information about telephone toll calls: the name, address, and telephone number of the caller, telephone number called, date, time and length of the call. Each carrier shall retain this information for toll calls that it bills whether it is billing its own toll service customers for toll calls or billing customers for another carrier.

[51 FR 39536, Oct. 29, 1986]

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996	)	CC Docket No. 96-115
	)	
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	)	
	)	
	)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information	)	RM-11277

COMMENTS OF THE UNITED STATES
DEPARTMENTS OF JUSTICE AND HOMELAND SECURITY

I. Introduction

The United States Department of Justice ("DOJ")[1] and the United States Department of Homeland Security ("DHS")[2] (collectively, "the Departments") hereby submit these comments on the Commission's *Notice of Proposed Rulemaking* ("*Notice*") in the above-captioned docket.[3] The Departments submit these comments to assist the Commission in its development of further rules protecting the privacy of customer

---

1 DOJ includes its constituent components, including the Federal Bureau of Investigation ("FBI") and the Drug Enforcement Administration ("DEA").

2 DHS includes its constituent law enforcement components, including the United States Secret Service and Immigration and Customs Enforcement.

3 *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, Notice of Proposed Rulemaking, CC Docket No. 96-115, RM-11277, FCC 06-10 (rel. Feb. 14, 2006).

proprietary network information ("CPNI") without sacrificing lawful access to important information that helps solve crimes, prevent terrorist attacks, and safeguard our national security.

This proceeding was initiated primarily in response to a Petition for Rulemaking filed by the Electronic Privacy Information Center ("EPIC") that raised concerns about the sufficiency of carrier practices related to CPNI.[4] Among other things, EPIC recommended that the Commission adopt rules requiring that call detail records be destroyed when they are no longer needed for billing or dispute purposes or, in the alternative, requiring carriers to "de-identify" identification data from the transactional records.[5] In the *Notice*, the Commission requested comment on "whether CPNI records should eventually be deleted, and if so, for how long such records should be kept."[6] In exploring the potential negative consequences of a record destruction mandate, the Commission has asked whether "deleting CPNI or removing personal identification conflict with other priorities, such as . . . law enforcement."[7]

The answer to the above question is an unequivocal "yes," and we urge the Commission to explore ways to resolve the issues EPIC has raised in ways that preserve lawful access to communications records and other CPNI. For law enforcement, such CPNI is an invaluable investigative resource, the mandatory destruction of which would severely impact the Departments' ability to protect national security and public safety.

---

4 Petition of the Electronic Privacy Information Center for Rulemaking to Enhance the Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005) ("EPIC Petition").

5 *See* EPIC Petition at 11-12.

6 *Notice* ¶ 20.

7 *Id.*

As reflected in prior Commission filings on CPNI issues, the Departments fully support the Commission's goal of protecting the privacy and security of CPNI through rules prescribing the proper use and handling of that very sensitive information.[8] But while measures are needed to prevent *improper* access to this sensitive information, such measures should not work to limit properly authorized officials from lawfully accessing CPNI in order to solve and prevent crimes and to protect national security and public safety. In crafting any solution to the problems raised by the EPIC Petition, the Departments urge the Commission to reject imposing a mandate to destroy invaluable information used by the Departments in many of their most important investigations.[9]

II. The Commission's Rules Should Focus On Proper Security For All CPNI, Not On A Mandatory Destruction Requirement That Fails To Protect Some Records And Frustrates Lawful Access To Others.

---

[8] *See, e.g.*, Reply Comments of the United States Department of Justice and the Federal Bureau of Investigation, *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Third Further Notice of Proposed Rulemaking, CC Docket No. 96-115 at 4, n. 8 (filed Nov. 19, 2002); Comments of the Federal Bureau of Investigation, *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Notice of Proposed Rulemaking, CC Docket No. 96-115 (filed Jul. 9, 1997); Comments of the Federal Bureau of Investigation, *In the Matter of 1998 Biennial Regulatory Review of International Common Carrier Regulations*, Notice of Proposed Rulemaking, IB Docket No. 98-118 (filed Aug. 13, 1998).

[9] EPIC's alternative recommendation – record de-identification – is also an unworkable option with respect to law enforcement's lawful access to such records. De-identification would separate the data that identify a particular caller or recipient (e.g., name, address, numbers called, etc.) from the general transaction records. Because the data that identifies a particular caller or recipient is often the critical portion of the call record for investigatory purposes, an irreversible de-identification approach would undermine the usefulness of the information provided pursuant to legal access. Accordingly, mandating the de-identification of such records would be the equivalent of mandating their destruction for law enforcement investigatory purposes. A de-identification approach should therefore be rejected for the same reasons.

A mandatory destruction requirement is the wrong approach for two reasons. First, because not all records would be immediately destroyed, efforts are better focused on proper security for the records while they are maintained. Second, and more importantly, the inability to produce records in response to lawful authority would have a significant negative impact on national security and public safety. Accordingly, the Departments urge the Commission to focus on security measures to protect all CPNI against *unauthorized* access rather than a rule that would also preclude lawfully authorized access.

As the Commission recognized when it explicitly asked about the impact of EPIC's records destruction proposal on other concerns, CPNI has other valid uses, such as fraud prevention and the protection of a carrier's own network.[10] Another legally authorized use is to investigate crime and protect national security and public safety. The Departments seek lawful access to CPNI in connection with investigations of all kinds – from child pornography to illegal drug trafficking, counter-intelligence, espionage, and more. In fact, as the FBI has previously advised the Commission, lawfully-obtained CPNI is used in virtually every federal, state, and local investigation of consequence.[11] Such CPNI is critically important not only in solving crimes but also in preventing crimes and even saving lives.[12] As discussed below, the same is true in the national security and

---

[10] The Departments submit that, beyond any retention period required by law, carriers should be free to retain voluntarily CPNI for other legal and appropriate purposes, such as protecting their networks and mitigating fraud.

[11] *See* Comments of the Federal Bureau of Investigation, *in re Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115 (filed Jul. 9, 1997) at 5.

[12] *Id.*

espionage contexts, where lawfully-obtained CPNI has enabled law enforcement and national security agencies to prevent terrorist acts and acts of espionage.[13] The courts have likewise long recognized the importance of telephone records to the administration of justice – both to law enforcement in the investigation and prosecution of serious offenses, such as illegal drug trafficking and organized crime, and to defendants in establishing an alibi defense.[14] Thus, a mandatory destruction requirement – particularly one tied to a point in time completely unrelated to these purposes, i.e., when records cease to be "needed for billing or dispute purposes" – would inevitably result in the loss of critical information to many such investigations and cases.[15]

Moreover, a mandatory records destruction regime would be particularly inappropriate, because it could hinder efforts to counter international terrorism. Lawful access to communications records is a critical tool in the fight against global terrorism. Such records, when combined with other investigative information, can be used to establish the movements and identities of known and suspected terrorists. Mobile phone records, for example, were instrumental in tracking down the perpetrators of the Madrid

---

13 *Id.* at 6-7.

14 *See, e.g. U.S. v. Hanardt*, 173 F. Supp. 2d 801 (N.D. Ill. 2001) (phone records helped establish defendant's "long-time connection to Chicago organized crime"); *U.S. v. Scala*, 388 F. Supp. 2d 396 (S.D.N.Y. 2005) (cellular phone records showed numerous calls between defendant and known organized crime figures); *Reporters Committee for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1036-37 (D.C. Cir. 1978) (noting that "toll-billing records have become an invaluable law enforcement aid" and that information from toll-billing records has been used by state and federal law enforcement officials in criminal investigations and prosecutions for over 50 years). *See also Butler v. State*, 716 S.W.2d 48 (Tex. Crim. App. 1986) (telephone toll record was the key factor in establishing alibi defense).

15 We note that any mandatory data destruction requirement would also largely negate the utility of the existing data preservation scheme under 18 U.S.C. § 2703(f); if the data relating to a specific investigation has been destroyed, there will be nothing for providers to preserve in response to a request from law enforcement.

bombings that killed 191 and injured approximately 1,800 people on March 11, 2004.[16] The National Commission on Terrorist Attacks Upon the United States also relied on telephone records in numerous instances to establish the movements and contacts of the 9/11 hijackers before their terrorist attacks on the World Trade Center and the Pentagon on September 11, 2001.[17]

It is precisely these kinds of concerns that motivated the Commission to abandon its former rules requiring data destruction and adopt its current rules that require the maintenance of certain categories of CPNI. Prior to 1986, the Commission's Part 42 carrier record-keeping rules required, among other things, that carriers (1) macerate or destroy the legibility of records the contents of which are forbidden by law to be divulged to unauthorized persons,[18] and (2) retain telephone toll records for six months.[19] As part of a comprehensive review by the Commission of its Part 42 rules and in response to a related request by DOJ to extend the telephone toll record retention period specified therein, the Commission (among other things) eliminated the records destruction

---

16 *See* "Madrid Bombing 'Manager' in Court," BBC News (June 3, 2005), viewable at http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/england/berkshire/4607175.stm (telephone records used to show bombing "manager" had been in contact with people involved in the Madrid bombings).

17 *See The 9/11 Commission Report* (released Jul. 22, 2004) at 217, 515 n.26, 522 n.68.

18 *See In the Matter of Revision of Part 42, Preservation of Records of Communication Common Carriers*, Notice of Proposed Rulemaking, 1985 FCC LEXIS 2945 ¶¶ 13, 23 (1985) ("*Part 42 NPRM*") (discussing the record destruction requirement contained in the then-current version of Section 42.6 of the Commissions rules, 47 C.F.R. § 42.6 (Destruction of Records) (1985)).

19 *See Part 42 NPRM* ¶ 18 (discussing the toll record retention requirement contained in the then-current version of Section 42.9 of the Commissions rules, 47 C.F.R. § 42.9 (List of Records) (1985)).

requirement and extended the toll record retention period to 18 months.[20] In granting DOJ's request, the Commission specifically recognized that an extension of the retention period was warranted in order to "support successful investigations and prosecutions . . . ."[21] In extending the retention period, the Commission – with DOJ's input – refined and narrowed the specific information that law enforcement stated it would need to support its investigative efforts at that time.[22]

In addition to the Commission's own prior acknowledgment of the difficulties a destruction requirement presents, recent experience in other countries further highlights the problems created by such requirements. The establishment of a data destruction regime in the European Union ("EU") a number of years ago has been found to be incompatible with protection of public safety and national security. In response, the EU recently adopted a Directive – binding on all of its member countries – that will have the effect of mandating all "providers of publicly available communications services" to

---

20 *See In the Matter of Revision of Part 42, Preservation of Records of Communication Common Carriers*, Report and Order, 1986 WL 290829, 60 Rad. Reg. 2d (P&F) 1529 ¶¶ 4, 23-27, 38, 41-42 (1986) ("*Part 42 Order*"). DOJ's request was supported by the Advisory Committee for United States Attorneys, the FBI, the Bureau of Alcohol, Tobacco and Firearms, the U.S. Postal Service, and the Immigration and Naturalization Service. *See Part 42 NPRM* ¶ 18.

21 *See Part 42 Order* ¶ 41.

22 *See Part 42 Order* ¶ 43. The specific information that DOJ indicated law enforcement would need at that time includes the name, address, and telephone number of the caller; telephone number called; the date, time, and length of the call; and automatic message accounting tapes. *Id.* The list of law enforcement-required information was incorporated into Section 42.6 of the Commission's rules and remains listed therein today. *See* 47 C.F.R. § 42.6 (2006).

store and retain communications data for up to two years.[23] In acknowledging the need for data retention requirements, the EU Parliament and Council recognized that:

> retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive.[24]

EPIC's recommended data destruction mandate would cause the Commission to regress to a course it has long since rejected. If anything, reliance on telephone call records as an investigative resource to protect public safety and national security has only increased and become more critical in the almost twenty years since the Commission revised Section 42.6 of its rules to extend the telephone records retention period.[25] Notwithstanding this increased reliance on such records, however, the efficacy of the Commission's current Section 42.6 requirement to meet law enforcement needs has been significantly eroded.

While the risks are clear and many, the benefit from a mandatory destruction requirement is largely unclear and certainly limited. The mandatory destruction of some

---

23 *See* Council Directive, 2006/24/EC, 2006 O.J. (L 105) 54, Article 6 ("Directive"), viewable at http://europa.eu.int/eur-lex/lex/JOHtml.do?uri=OJ:L:2006:105:som:en:html. *See also* Miriam H. Wugmeister and Karin Retzer, *Data Retention – Implications for Business*, 7 NO. 2 Privacy & Info. L. Rep. 7 (2006).

24 *See* Directive at 4 ¶ 9.

25 Moreover, as the Commission notes in the *Notice*, carriers themselves have already expressed concern about potential conflicts with Commission rules that require that call records and other CPNI be kept for at least a minimum period of time. *See Notice* ¶ 20 (noting carriers' comments that destroying records might conflict with the Commission's Part 42 record-keeping rules, 47 C.F.R. §42.01-11).

CPNI does nothing to address a significant portion of CPNI, specifically information needed for billing disputes, which will still need to be secured.[26] In fact, the material retained will most likely be the most recent records and hence possibly the most useful for data brokers. Rather than expending effort on promulgating rules with significant omissions, the Commission should instead focus its efforts, and those of carriers, on appropriate security measures that ensure that any access to such records is done only with valid legal authority. As the Department of Justice has urged the Commission for years, one large step in that direction would be to require that CPNI of U.S. customers of domestic services be stored exclusively within the United States.[27]

In opposing and pointing out the inadequacies of a data destruction regime, the Departments do not thereby imply that the current CPNI rules are adequate effectively to meet law enforcement's needs or protect public safety and national security. As noted above, the Departments have previously asked the Commission to strengthen the security of these records in a number of ways.[28] Further, developments in the world and in the communications marketplace since the Commission's last examination of these rules have highlighted the limited scope of the Commission's rules. Today, many modern

---

[26] The statute of limitations in Section 415 of the Communications Act for billing disputes is two years. 47 U.S.C. § 415. The nature of Section 415 necessarily compels carriers to maintain all potentially relevant documents needed in connection with resolving actions concerning recovery of lawful charges or damages.

[27] *See* Reply Comments of the United States Department of Justice and the Federal Bureau of Investigation, *In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* Third Further Notice of Proposed Rulemaking, CC Docket No. 96-115 at 4, n.8 (filed Nov. 19, 2002).

[28] *See id. See also* Comments of the United States Department of Justice, *In the Matter of IP-Enabled Services,* Notice of Proposed Rulemaking, WC Docket No. 04-36 (filed May 28, 2004).

communications service providers maintain sensitive records about their customers' private communications, yet these new carriers have not been made subject to the rules that have traditionally governed CPNI.[29] In addition, as carriers covered by the Commission's existing rules have increasingly moved away from classic billing models, in which charges are itemized and billed by type of service, to non-measured, bundled, and flat-rate service plans, some carriers have claimed that call records under such new plans are not covered by Section 42.6 because they are not "toll records." Therefore, these carriers have argued that no records need be retained. This has significantly diminished the availability of call records that were historically made available to law enforcement, pursuant to lawful process, as traditional "billing records" under the Commission's rules. While it is recognized that changes in the communications industry over the past decade have resulted in changes in the record retention practices of such providers, it must also be acknowledged that the nature and immediacy of the threat confronting public safety and national security has significantly changed and evolved such that the need lawfully to access these critical records has increased, not diminished.

As a consequence of these changes, the Departments believe it is necessary to re-examine the Commission's existing rules which no longer fulfill critical public safety or national security needs in three key respects: 1) the scope of carriers and providers

---

[29] *Id.* To the extent that the *Notice* requests comment on whether any requirements that the Commission might adopt in the present rulemaking should extend to VoIP or other IP-enabled service providers, the Departments refer to their May 28, 2004 comments on this subject.

covered; 2) the scope of information and records covered, and; 3) the duration of retention of information and records.[30]

The critical role that communications records play in the Departments' most important investigations and the serious consequences for public safety and national security which result from the unavailability of such records cannot be understated. The Attorney General recently underscored this point when he noted that the investigation and prosecution of child predators depends critically on the availability of evidence that is often in the hands of Internet service providers. He observed that this evidence will be available to law enforcement only if the providers retain the records for a reasonable amount of time. Consequently, the Attorney General asked experts at the Department of Justice to examine how the failure of some Internet service providers to keep such records has hampered the Department's efforts to investigate and prosecute child predators.[31] In recognition of the importance of this issue, the Departments each will be evaluating how the availability of different categories of data held by different types of modern communications carriers impacts the Departments' respective missions. In addition, the Attorney General has pledged to reach out personally to leading service providers and other industry leaders to solicit their input and assistance. As these efforts develop, the Departments expect to have further views on how long data should be held, what data should be retained, and which carriers should have such obligations.

---

[30] It should be noted that whereas the Commission has limited the retention period for toll records to 18 months, the statute of limitations for many federal felony crimes is five years, during which time law enforcement needs for relevant evidence continue. The Commission should explore, with further input from law enforcement, the degree to which the existing 18-month rule should be extended.

[31] *See* Prepared Remarks of Attorney General Alberto R. Gonzales at the National Center for Missing and Exploited Children (NCMEC) in Alexandria, Virginia, on April 20, 2006, available at http://www.usdoj.gov/ag/speeches/2006/ag_speech_060420.html.

III. Any Notice Requirement Adopted by the Commission Should Include A Provision Requiring Advance Notice to Law Enforcement and, Where Appropriate, Delayed Notice To The Consumer.

The EPIC Petition also suggested that carriers should be required to notify affected customers when there has been an improper disclosure of CPNI.[32] In the *Notice*, the Commission went further and asked for comments regarding "the costs and benefits of routinely notifying customers after any release of their CPNI."[33] While the Departments strongly support prompt victim notification in the case of security breaches, we believe any rule requiring such notification should also require that carriers first notify law enforcement authorities and, where appropriate, allow law enforcement to request a reasonable delay in notification to the consumer where such notification might harm related law enforcement investigative efforts. In addition, any requirement that customers routinely be notified of disclosures of their CPNI should make clear that it does not alter the rules already established by Congress regarding the circumstances under which a customer must be notified of law enforcement access to customer records.

Requiring advance notice to law enforcement of security breaches, together with the option of delaying consumer notification, can serve several important goals. First, anecdotal evidence suggests that many CPNI breaches go unreported to law enforcement. Only by prompt investigation of such breaches can the offenders be identified and punished. Thus, required reporting to law enforcement will deter further breaches of CPNI security. Second, where deemed necessary by law enforcement, a reasonable delay can help preserve evidence critical to the investigation of misappropriation of CPNI. If a carrier suffering an intrusion or theft must immediately announce the security breach to

---

32 *See* EPIC Petition at 11.

affected customers and to the public, the persons responsible may be tipped off that law enforcement is investigating their crime. Criminals would then have the opportunity to destroy evidence, change their behavior, and otherwise jeopardize the investigation and avert justice. Indeed, the approach outlined above is the one taken by a variety of proposed legislation currently under consideration by Congress.[34]

The Commission's questions regarding routine notification of any access to CPNI, even when no security breach is suspected, raise additional issues.[35] There may be good reasons that a carrier may want to disclose CPNI without notifying its customer, e.g., during the course of a fraud investigation. But if the Commission does decide to go beyond notification of actual security breaches, it should at a minimum make clear that any new requirements do not alter the balance struck by Congress for when law enforcement access to customer records must be disclosed. *See* 18 U.S.C. 2701 *et seq.* Because Congress has already established a structure for customer notification of law enforcement access to customer records, the Commission should exclude disclosure of CPNI to law enforcement from any routine notification requirement.

IV. Conclusion

For the reasons stated herein, the Departments urge the Commission not to adopt rules mandating the destruction of call records and similar CPNI, a vitally important investigative resource for protecting public safety and national security. Such a rule would undoubtedly hinder the Departments' ability to carry out their respective public

---

33 *Notice* ¶ 23.

34 *See, e.g.*, Data Accountability and Trust Act, H.R. 4127, 109th Cong. (2005); Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong. (2005).

35 *Notice* ¶ 23.

safety and national security responsibilities. Additionally, the Departments suggest that any new rules requiring customer notification in the case of improper CPNI disclosure include a requirement that carriers provide prompt notice to law enforcement and an opportunity for law enforcement to request delayed notification to the consumer. We appreciate the Commission's recognition and support of the Departments' important mission in these areas.

Dated: April 28, 2006

Respectfully submitted,

THE UNITED STATES DEPARTMENT OF JUSTICE

/s/ Laura H. Parsky
Laura H. Parsky
Deputy Assistant Attorney General
Criminal Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Room 2113
Washington, D.C. 20530
(202) 616-3928

and

/s/ Elaine N. Lammert
Elaine N. Lammert
Deputy General Counsel
Office of the General Counsel
Federal Bureau of Investigation
United States Department of Justice
J. Edgar Hoover Building
935 Pennsylvania Avenue, N.W.
Room 7435
Washington, D.C. 20535
(202) 324-1530

and

/s/ Michael L. Ciminelli

Michael L. Ciminelli
Deputy Chief Counsel
Office of Chief Counsel
Drug Enforcement Administration
United States Department of Justice
Washington, D.C. 20537
(202) 307-8020

and

THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY

/s/ Stewart A. Baker

Stewart A. Baker
Assistant Secretary for Policy
United States Department of Homeland Security
3801 Nebraska Avenue, N.W.
Washington, D.C. 20528
(202) 282-8030

~~SECRET~~

b6
b7C

From: [redacted](OGC) (FBI)
Sent: Thursday, September 07, 2006 9:45 AM
To: [redacted](OGC) (FBI); [redacted]DI) (FBI); [redacted]; [redacted](OGC) (FBI); [redacted]; [redacted]OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted]; [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted]; [redacted]OGC) (FBI)
Subject: FW: NSL enforcement issue\\ Billing Records \ 47 CFR 42.6 \ HIPPA
UNCLASSIFIED
NON-RECORD

fyi

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted]

b6
b7C
b2

Unit Chief
National Security Law Policy and Training Unit
FBI HQ Room 7975
STU III: [redacted]
Unclassified Fax: [redacted]
Secure Fax: [redacted]

DATE: 06-09-2007
CLASSIFIED BY 65179 DMH/KSR/JW
REASON: 1.4 (C)
DECLASSIFY ON: 06-09-2032

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Wednesday, September 06, 2006 7:34 PM
To: [redacted](OGC) (FBI); [redacted](OGC) (FBI)
Cc: [redacted](OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); [redacted](OGC) (FBI); LAMMERT, ELAINE N. (OGC) (FBI)
Subject: RE: NSL enforcement issue\\ Billing Records \ 47 CFR 42.6 \ HIPPA

b6
b7C

UNCLASSIFIED
NON-RECORD

b1
b6
b7C
b5

[redacted]

(S)

~~SECRET~~

SECRET


CPNINPRMCOMMEN TS(4-28-06FINAL)... 47 CFR 42-6_Tel Billing Record...

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
b6 **Engineering Research Facility**
b7C [redacted]
Quantico, VA 22135
Tel.
Fax [redacted]

DATE: 06-09-2007
CLASSIFIED BY 65179 DMH/KSR/JW
REASON: 1.4 (C)
DECLASSIFY ON: 06-09-2032

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

-----Original Message-----
b6 **From:** [redacted] (OGC) (FBI)
b7C **Sent:** Wednesday, September 06, 2006 12:22 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: FW: NSL enforcement issue

~~UNCLASSIFIED~~
~~NON-RECORD~~

(S)

[redacted]

b1
b5
b6
b7C

-----Original Message-----
b6 **From:** [redacted] (OGC) (FBI)
b7C **Sent:** Wednesday, September 06, 2006 11:52 AM
To: [redacted] (OGC) (FBI)

SECRET

SECRET

Subject: RE: NSL enforcement issue

UNCLASSIFIED
NON-RECORD

b5 [redacted]

Julie

-----Original Message-----
b6 **From:** [redacted] (OGC) (FBI)
b7C **Sent:** Tuesday, September 05, 2006 6:05 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Subject: RE: NSL enforcement issue

UNCLASSIFIED
NON-RECORD

b5 [redacted]

-----Original Message-----
b6 **From:** THOMAS, JULIE F. (OGC) (FBI)
b7C **Sent:** Tuesday, September 05, 2006 3:11 PM
To: [redacted] OGC) (FBI)
Subject: RE: NSL enforcement issue

UNCLASSIFIED
NON-RECORD

b5 [redacted]

Julie

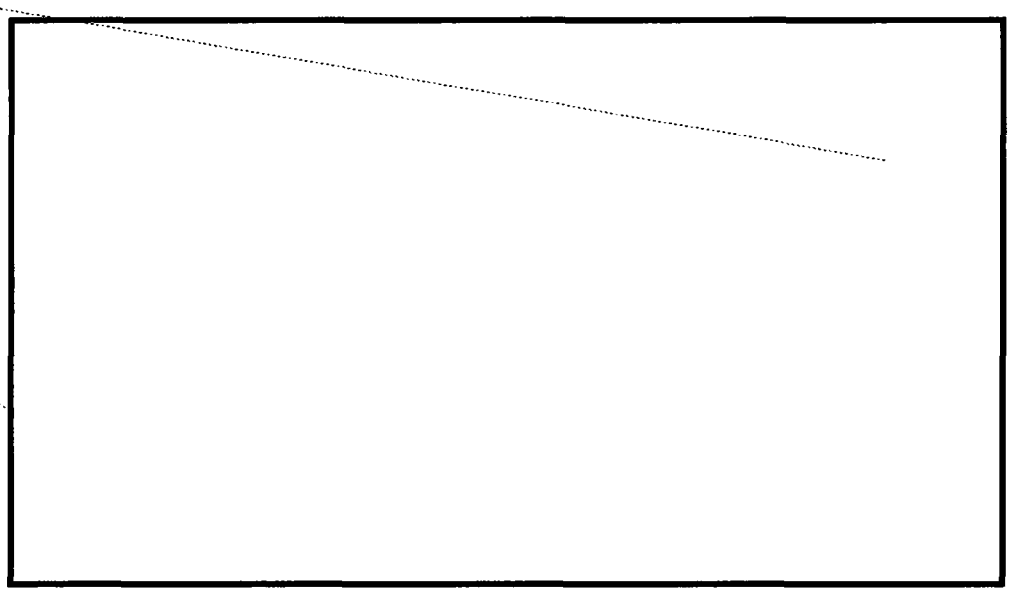
-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Friday, September 01, 2006 8:06 AM
To: [redacted] (OGC) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI) [redacted] (FBI)
Subject: NSL enforcement issue

b6
b7C **SENSITIVE BUT UNCLASSIFIED**
NON-RECORD

SECRET

SECRET

(S)



b1
b5
b6
b7C (S)

SENSITIVE BUT UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

SECRET

[Code of Federal Regulations]
[Title 47, Volume 3]
[Revised as of October 1, 2005]
From the U.S. Government Printing Office via GPO Access
[CITE: 47CFR42.6]

[Page 6]

TITLE 47--TELECOMMUNICATION

CHAPTER I--FEDERAL COMMUNICATIONS COMMISSION (CONTINUED)

PART 42_PRESERVATION OF RECORDS OF COMMUNICATION COMMON CARRIERS--Table
of Contents

Sec. 42.6 Retention of telephone toll records.

Each carrier that offers or bills toll telephone service shall retain for a period of 18 months such records as are necessary to provide the following billing information about telephone toll calls: the name, address, and telephone number of the caller, telephone number called, date, time and length of the call. Each carrier shall retain this information for toll calls that it bills whether it is billing its own toll service customers for toll calls or billing customers for another carrier.

[51 FR 39536, Oct. 29, 1986]

MessageFrom: (OGC) (FBI)
Sent: Thursday, August 04, 2005 8:40 AM
To: (OGC) (FBI); (DI) (FBI); (OGC) (FBI); (OGC) (FBI); (OGC) (FBI); (CTD) (FBI); (OGC) (FBI); (OGC) (FBI); (OGC) (FBI); (OGC) (FBI); (OGC) (FBI); (OGC) (FBI); L (OGC) (FBI)
Cc: BOWMAN, MARION E. (OI) (FBI); (OGC)(FBI)
Subject: FW: 2709 Attachment

UNCLASSIFIED
NON-RECORD

b6
b7C

b5
b6
b7C

Unit Chief
National Security Law Policy and Training Unit
FBI HQ Room 7975
STU III:
Unclassified Fax:
Secure Fax:

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-08-2007 BY 65179 DMH/KSR/JW

-----Original Message-----
From: (OGC)(FBI)
Sent: Wednesday, August 03, 2005 11:10 AM
To: (OGC) (FBI); (OGC) (FBI)
Subject: 2709 Attachment

UNCLASSIFIED
NON-RECORD

FYI

Assistant General Counsel
National Security Law Branch
Office of General Counsel FBI
Voice
Pager
Secure Fax
Fax

UNCLASSIFIED

UNCLASSIFIED

b6
b7C
b5

From: [redacted](OGC) (FBI)
Sent: Thursday, December 14, 2006 1:11 PM
To: [redacted](OGC) (FBI); [redacted](DI) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI)
Subject: FW: Draft NSL EC - [redacted]

UNCLASSIFIED
NON-RECORD

You should read the attached EC.

b6
b7C
b2

[redacted]
Unit Chief
National Security Law Policy and Training Unit
FBI HQ Room 7975
STU II [redacted]
Unclassified Fax: (202) [redacted]
Secure Fax: (202 [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-09-2007 BY 65179 DMH/KSR/JW

-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Wednesday, December 13, 2006 12:48 PM
To: [redacted](OGC) (FBI)
Cc: [redacted](OGC) (FBI); [redacted](OGC) (FBI)
Subject: FW: Draft NSL EC - [redacted]

b6
b7C
b5

UNCLASSIFIED
NON-RECORD

I made some edits and asked a question.

Julie

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Monday, December 11, 2006 4:29 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Cc: [redacted](OGC) (FBI); [redacted](OGC) (FBI)
Subject: Draft NSL EC - [redacted]

b6
b7C
b5

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b5 [redacted]

NSLmiscellaneousEC
.wpd (24 KB)...

SENSITIVE BUT UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

b6
b7C

From: [redacted] (OGC) (FBI)
Sent: Thursday, September 07, 2006 9:45 AM
To: [redacted] (OGC) (FBI); [redacted] (DI) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: FW: NSL enforcement issue\\ Billing Records \ 47 CFR 42.6 \ HIPPA

~~UNCLASSIFIED~~
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

fyi

[redacted]

Unit Chief
National Security Law Policy and Training Unit
FBI HQ Room 7975
STU III: (202) [redacted]
Unclassified Fax: (202) [redacted]
Secure Fax: (202) [redacted]

b6
b7C
b2

DATE: 06-09-2007
CLASSIFIED BY 65179 DMH/KSR/JW
REASON: 1.4 (C)
DECLASSIFY ON: 06-09-2032

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, September 06, 2006 7:34 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); [redacted] (OGC) (FBI); LAMMERT, ELAINE N. (OGC) (FBI)
Subject: RE: NSL enforcement issue\\ Billing Records \ 47 CFR 42.6 \ HIPPA

b6
b7C

~~UNCLASSIFIED~~
NON-RECORD

b5
b1
b6
b7C

(S) [redacted]

SECRET


CPNINPRMCOMMEN TS(4-28-06FINAL)... 47 CFR 42-6_Tel Billing Record...

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
[redacted]
Quantico, VA 22135
Tel.
Fax [redacted]

b6
b7C
b2

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, September 06, 2006 12:22 PM
To: [redacted] (OGC) (FBI) [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: FW: NSL enforcement issue

b6
b7C

UNCLASSIFIED
NON-RECORD

(S) [redacted]

b1
b5
b6
b7C

-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Wednesday, September 06, 2006 11:52 AM
To: [redacted] (OGC) (FBI)

b6
b7C

SECRET

SECRET

Subject: RE: NSL enforcement issue

UNCLASSIFIED
NON-RECORD

b5 [redacted]

Julie

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Tuesday, September 05, 2006 6:05 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Subject: RE: NSL enforcement issue

b6
b7C

UNCLASSIFIED
NON-RECORD

b5 [redacted]

-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Tuesday, September 05, 2006 3:11 PM
To: [redacted] (OGC) (FBI)
Subject: RE: NSL enforcement issue

b6
b7C

UNCLASSIFIED
NON-RECORD

b5 [redacted]

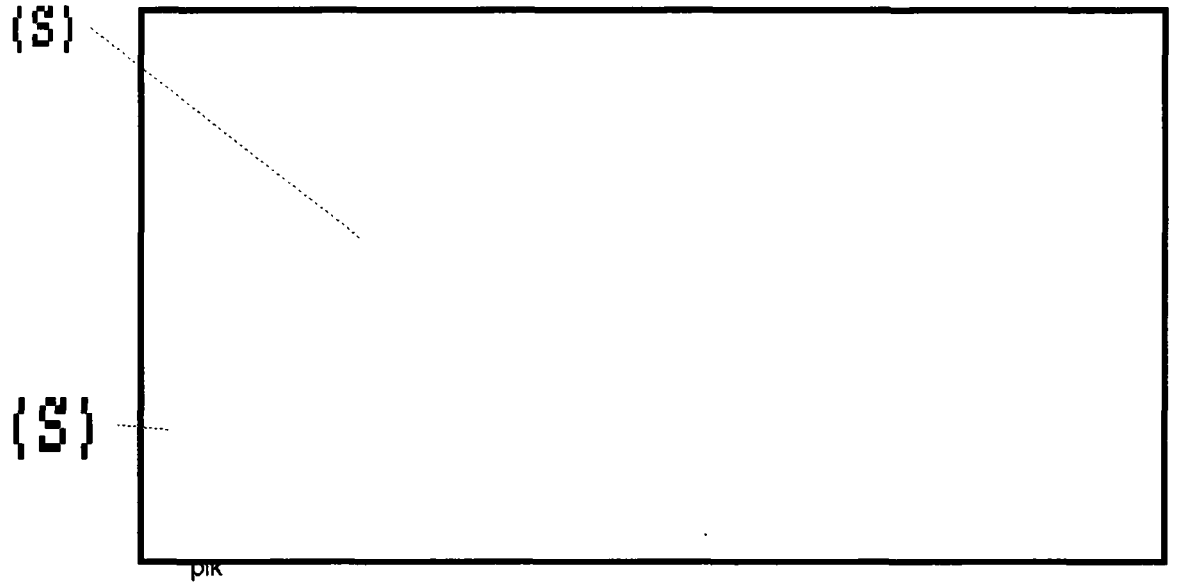
Julie

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Friday, September 01, 2006 8:06 AM
To: [redacted] (OGC) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI); [redacted] (FBI)
Subject: NSL enforcement issue

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

SECRET



b5
b1

~~SENSITIVE BUT~~ UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

~~SECRET~~

b6
b7C

From: [redacted] (OGC) (FBI)
Sent: Wednesday, September 06, 2006 4:15 PM
To: [redacted] (OGC) (FBI); [redacted] (DI) (FBI); [redacted]; [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: FW: NSL enforcement issue

~~UNCLASSIFIED~~
~~NON-RECORD~~

b6
b7C
b2

[redacted] brings up very important issues on NSLs.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Unit Chief
National Security Law Policy and Training Unit
FBI HQ Room 7975
STU III: (202) [redacted]
Unclassified Fax: (202) [redacted]
Secure Fax: (202) [redacted]

DATE: 06-09-2007
CLASSIFIED BY 65179 DMH/KSR/JW
REASON: 1.4 (C)
DECLASSIFY ON: 06-09-2032

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, September 06, 2006 12:22 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: FW: NSL enforcement issue

b6
b7C

~~UNCLASSIFIED~~
~~NON-RECORD~~

(S)

[redacted]

b1
b5
b6
b7C

-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Wednesday, September 06, 2006 11:52 AM

~~SECRET~~

~~SECRET~~

b6
b7C

To: [redacted] (OGC) (FBI)
Subject: RE: NSL enforcement issue

~~**UNCLASSIFIED**~~
NON-RECORD

b1
b5

[redacted]

Julie

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Tuesday, September 05, 2006 6:05 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Subject: RE: NSL enforcement issue

b6
b7C

~~**UNCLASSIFIED**~~
NON-RECORD

b5

[redacted]

-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Tuesday, September 05, 2006 3:11 PM
To: [redacted] (OGC) (FBI)
Subject: RE: NSL enforcement issue

b6
b7C

~~**UNCLASSIFIED**~~
NON-RECORD

b5

[redacted]

Julie

-----Original Message-----
From: [redacted] OGC) (FBI)
Sent: Friday, September 01, 2006 8:06 AM
To: [redacted] OGC) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI); [redacted] (FBI)
Subject: NSL enforcement issue

b6
b7C

~~**SENSITIVE BUT UNCLASSIFIED**~~
NON-RECORD

~~SECRET~~

~~SECRET~~

(S)

b5
b1
b6
b7C

(S)

~~SENSITIVE BUT UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~SECRET~~

~~SECRET~~

From: [redacted] (OGC) (FBI)
Sent: Tuesday, August 08, 2006 5:19 PM
b6 **To:** [redacted] (OGC) (FBI); [redacted] (FBI); [redacted]
b7C [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: b5 FW: [redacted]

Importance: High
~~SECRET//ORCON,NOFORN~~
RECORD NSL

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

I will discuss this at our unit meeting.

[redacted]
b6 **Unit Chief**
b7C **National Security Law Policy and Training Unit**
FBI HQ Room 7975
b2 **STU III: (202) [redacted]**
Unclassified Fax: (202) [redacted]
Secure Fax: (202) [redacted]

DATE: 06-09-2007
CLASSIFIED BY 65179 DMH/KSR/JW
REASON: 1.4 (C)
DECLASSIFY ON: 06-09-2032

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Tuesday, August 08, 2006 2:57 PM
b6 **To:** THOMAS, JULIE F. (OGC) (FBI); CAPRONI, VALERIE E. (OGC) (FBI)
b7C **Cc:** [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (FBI); [redacted] (OGC) (FBI)
b5 **Subject:** [redacted]
Importance: High

~~SECRET//ORCON~~,NOFORN
RECORD NSL

(S) Julie & Valerie-- I have been advised by SAC Art Cummings [redacted]

b1
b5
b2
b7E [redacted]

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence

~~SECRET~~

Investigations
DECLASSIFICATION EXEMPTION 1
SECRET//ORCON,NOFORN

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET//ORCON,NOFORN

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

b6
b7C

Precedence: ROUTINE **Date:** 12/15/2006

To: Can Valerie signout an all Division EC?
Attn: ADIC/SAC

CDC

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

b6
b7C

Approved By:
Caproni Valerie E
Thomas Julie F

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 06-19-2007 BY 65179 DMH/KSR/JW

Drafted By: [redacted] pik

Case ID #: (U) 319X-HQ-A1487720-OGC

1073946

Title: (U) LEGAL ADVICE AND OPINIONS;
UPLOADING OF NSL RETURN INFORMATION

Synopsis: (U) Provides guidance to the field as to the need to review NSL return information prior to uploading the information into FBI databases.

Details: (U)

It has come to the attention of the Office of General Counsel, National Security Law Branch (NSLB), that there may be occasions in which NSL information has been uploaded into Telephone Applications and other databases prior to having been reviewed by any FBI personnel. This is particularly likely to occur if the information is received in electronic form. However, a problem arises if the information that was received is not responsive to the NSL and thus, not relevant to an authorized national security investigation, or, alternatively, if there was a mistake by the FBI in the NSL such that the records are responsive but not relevant to an authorized investigation. Such deficiencies in the NSL return information may never be discovered, or, discovered too late to prevent the use of information that the FBI did not properly collect. Therefore, it is imperative that the records be reviewed before uploading to assure that they are relevant to an authorized national security investigation. Thereafter, if the records were properly obtained,

they may be uploaded into a database. If there is a problem with the manner in which they were obtained, other steps need to be taken.[1]

Any questions about this matter may be directed to AGC [redacted] at 571[redacted]

b6
b7C
b2

1- Ms. Caproni
1- Ms. Thomas
1- [redacted]

[1] If the records were not properly obtained, i.e., there was a mistake by the carrier or the FBI in the NSL process, then the records should be sequestered with the CDC, and a potential IOB reported to NSLB. Thereafter, in its responsive EC, NSLB will indicate the proper disposition of the records. If the records were in fact properly obtained (e.g., the records are covered by the attachment, if not the body of the NSL)), they may be retained and uploaded. If the records were not properly obtained but are relevant to an authorized investigation (e.g., exceed the time frame of the NSL but pertain to the subject of the NSL), the records should remain sequestered until another NSL is issued to cover those records. If the records were not properly obtained and are not relevant to an authorized investigation, the CDC is expected to contact the owner of the records and determine if the entity wants the records returned to it or destroyed by the FBI. For a full explanation of the manner in which NSL records should be maintained for IOB purposes, see EC, dated 11/16/2006, 278-HQ-C1229736, serial 2570.

Freedom of Information and Privacy Acts

SUBJECT: NATIONAL SECURITY LETTERS
FOLDER: CTD | CD | Volume 15

Federal Bureau of Investigation

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ COVER SHEET

Total Deleted Page(s) ~ 65
Page 103 ~ Referral/Direct
Page 104 ~ Referral/Direct
Page 105 ~ Referral/Direct
Page 106 ~ Referral/Direct
Page 107 ~ Referral/Direct
Page 108 ~ Referral/Direct
Page 109 ~ Referral/Direct
Page 110 ~ Referral/Direct
Page 111 ~ Referral/Direct
Page 112 ~ Referral/Direct
Page 113 ~ Referral/Direct
Page 114 ~ Referral/Direct
Page 115 ~ Referral/Direct
Page 116 ~ Referral/Direct
Page 117 ~ Referral/Direct
Page 118 ~ Referral/Direct
Page 119 ~ Referral/Direct
Page 120 ~ Referral/Direct
Page 121 ~ Referral/Direct
Page 122 ~ Referral/Direct
Page 123 ~ Referral/Direct
Page 124 ~ Referral/Direct
Page 125 ~ Referral/Direct
Page 126 ~ Referral/Direct
Page 127 ~ Referral/Direct
Page 128 ~ Referral/Direct
Page 129 ~ Referral/Direct
Page 130 ~ Referral/Direct
Page 131 ~ Referral/Direct
Page 132 ~ Referral/Direct
Page 133 ~ Referral/Direct
Page 134 ~ Referral/Direct
Page 135 ~ Referral/Direct
Page 136 ~ Referral/Direct
Page 137 ~ Referral/Direct
Page 138 ~ Referral/Direct
Page 139 ~ Referral/Direct
Page 140 ~ Referral/Direct
Page 141 ~ Referral/Direct
Page 142 ~ Referral/Direct
Page 143 ~ Referral/Direct
Page 144 ~ Referral/Direct
Page 145 ~ Referral/Direct
Page 146 ~ Referral/Direct

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

Page 147 ~ Referral/Direct
Page 148 ~ Referral/Direct
Page 149 ~ Referral/Direct
Page 150 ~ Referral/Direct
Page 151 ~ Referral/Direct
Page 152 ~ Referral/Direct
Page 153 ~ Referral/Direct
Page 154 ~ Referral/Direct
Page 155 ~ Referral/Direct
Page 156 ~ Referral/Direct
Page 157 ~ Referral/Direct
Page 158 ~ Referral/Direct
Page 159 ~ Referral/Direct
Page 160 ~ Referral/Direct
Page 161 ~ Referral/Direct
Page 162 ~ Referral/Direct
Page 163 ~ Referral/Direct
Page 164 ~ Referral/Direct
Page 165 ~ Referral/Direct
Page 166 ~ Referral/Direct
Page 167 ~ Referral/Direct

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

1073946

Good morning Mr. Chairman, Ranking Member Smith, and Members of the Committee. It is my pleasure to appear before you today to discuss the recent report by Department of Justice's Office of the Inspector General (OIG) regarding the FBI's use of national security letters (NSLs). The OIG's report is a fair report that acknowledges the importance of NSLs to the ability of the FBI to conduct the national security investigations that are essential to keeping the country safe. Importantly, the OIG found no deliberate or intentional misuse of the national security letter authorities, Attorney General Guidelines or FBI policy. Nevertheless, the OIG review identified several areas of inadequate auditing and oversight of these vital investigative tools, as well as processes that were inappropriate. Although not intentionally, we fell short in our obligations to report to Congress on the frequency with which we use this tool and in the internal controls we put into place to make sure that it was used only in accord with the letter of the law. Director Mueller concluded from the OIG's findings that we must redouble our efforts to ensure that there is no repetition of the mistakes of the past in the use of these authorities and I share his commitment. I would also like to acknowledge the role of Congress and the effectiveness of congressional oversight in surfacing the deficiencies raised in this audit, which was called for in the USA PATRIOT Improvement and Reauthorization Act. The report made ten recommendations in response to the findings, designed to provide both the necessary controls over the issuance of NSLs and the creation and maintenance of accurate records. The FBI fully supports each recommendation and concurs with the Inspector General that, when implemented, these reforms will ensure full compliance with both the letter and the spirit of the authorities entrusted to the Bureau.

National Security Letters

National Security Letters generally permit us to obtain the same sort of documents from third party businesses that prosecutors and agents obtain in criminal investigations with grand jury subpoenas. Unlike grand jury subpoenas, however, NSL authority comes through several distinct statutes and they have specific rules that accompany them. NSLs have been instrumental in breaking up cells like the "Portland Seven," the "Lackawanna Six," and the "Northern Virginia Jihad." Through the use of NSLs, the FBI has traced sources of terrorist funding, established telephone linkages that resulted in further investigation and arrests, and arrested suspicious associates with deadly weapons and explosives. NSLs allow the FBI to link terrorists together financially, and pinpoint cells and operatives by following the money.

The NSL authority used most frequently by the FBI is that provided by the Electronic Communications Privacy Act (ECPA). Through an ECPA NSL, the FBI can obtain subscriber information for telephones and electronic communications and can obtain toll billing information and electronic communication transaction records. Significantly, the FBI cannot obtain the content of communications through an ECPA NSL. Although the exact numbers of ECPA NSLs remains classified, it is the most common NSL authority used.

Pursuant to the Right to Financial Privacy Act (RFPA), the FBI also has the authority to issue NSLs for financial records from a financial institution. RFPA NSLs are used commonly in connection with investigations of potential terror financing.

Pursuant to the Fair Credit Reporting Act, the FBI has the authority to issue three different, but related, types of NSLs to credit reporting agencies: an NSL pursuant to 15 U.S.C. 1681u(a) for the names of financial institutions with which the subject has or has had an account; an NSL pursuant to 15 U.S.C. 1681u(b) for consumer identifying information (name, address, former

addresses, employment and former employment); an NSL pursuant to 15 U.S.C. 1681v for a full credit report. Of all the FBI"s NSL authorities, only the last of the FCRA authorities is restricted to use only in international terrorism cases.

Finally, the FBI has the authority to issue NSLs pursuant to the National Security Act in the course of investigations of improper disclosure of classified information by government employees.

For the first 3 types of NSLs (ECPA, RFPA, FCRA) the NSL must include a certification by an authorized FBI employee that the material is being sought for an authorized national security investigation. That certification is slightly different in the case of a FCRA NSL for a full credit report, where the certification required is that the information is relevant to an international terrorism investigation.

The authority to issue an NSL lies at a senior level within the FBI. An NSL can be issued only by an official who ranks not lower than Special Agent in Charge or Deputy Assistant Director. All such officials are career government employees who are members of the Senior Executive Service. Procedurally, an agent or analyst seeking an NSL must prepare a document (an electronic communication or EC) in which the employee lays out the factual predicate for the request. The factual recitation must be sufficiently detailed so that the approving official can determine that the material sought is relevant to an investigation. Additionally, it needs to provide sufficient information concerning the underlying investigation so that reviewing officials can confirm that the investigation is adequately predicated and not based solely on the exercise of First Amendment rights. Finally, the EC includes a "lead" to the Office of the General Counsel (OGC) for purposes of Congressional reporting.

OIG Report

As directed by Congress, we endeavored to declassify as much information as possible concerning our use of NSLs in order to allow the maximum amount of public awareness of the extent of our use of the NSL tool consistent with national security concerns. To that end, for the first time the public has a sense of the frequency with which the FBI makes requests for data with national security letters. In the period covered by the report, the number of NSL requests has ranged from approximately 40,000 to 60,000 per year and we have requested information on less than 20,000 persons per year. For a variety of reasons that will be discussed below, those numbers are not exact. Nevertheless, they, for the first time, allow the public to get some sense of the order of magnitude of these requests; there are a substantial number of requests, but we are not collecting information on hundreds of thousands of Americans.

There are three findings by the OIG that are particularly disturbing, and it is those three findings that I wish to address this morning: (1) inaccurate reporting to Congress of various data points we are obligated to report relative to NSLs; (2) the use of so-called exigent letters that circumvented the procedures required by ECPA; and (3) known violations (both previously self-reported by FBI and not previously reported) of law and policy with regard to usage of NSLs.

Congressional Reporting

A finding of the report that particularly distresses me is the section that addresses the inaccuracies of the numbers we report to Congress. That responsibility lies with my division, and we did not do an acceptable job. The process for tabulating NSLs simply did not keep up with the volume. Although we came to that realization prior to the OIG report and are working on a technological solution, that realization came later than it should have.

At some point several years before my tenure at the FBI began, our process for tracking NSLs for Congressional reporting purposes shifted from a totally manual process, where NSL data was written on index cards, to a standalone Access database. This database is referred to in the OIG report as the OGC database. While the OGC database was a giant technological step forward from 3 x 5 index cards, it is not an acceptable system given the significant increase in use of NSLs since 9/11. First and foremost, the OGC database is not electronically connected to ACS, the system from which we derive the data. Instead, there is a manual interface between ACS and the OGC database. An OGC employee is responsible for taking every NSL lead that is sent to OGC and manually entering the pertinent information into the OGC database. Nearly a dozen fields must be manually entered, including the file number of the case in which the NSL was issued (typically 15 digits and alphanumeric identifiers).

Approximately a year ago we recognized that our technology was inadequate and began developing an automated system to improve our ability to collect this data. The system, in addition to improving data collection, will automatically prevent many of the errors in NSLs that we will discuss today. We are building an NSL system to function as a workflow tool that will automate much of the work that is associated with preparing NSLs and the associated paperwork. The NSL system is designed to require the user to enter certain data before the workflow can proceed and requires specific reviews and approvals before the request for the NSL can proceed. Through this process, the FBI can automatically ensure that certain legal and administrative requirements are met and that required reporting data is accurately collected. For example, by requiring the user to identify the investigative file from which the NSL is to be issued, the system will be able to verify the status of that file to ensure that it is still open and current (e.g. request date is within six months

of the opening or an extension has been filed for the investigation) and ensure that NSLs are not being requested out of control or administrative files. The system will require the user to separately identify the target of the investigative file and the person whose records are being obtained through the requested NSL, if different. This will allow the FBI to accurately count the number of different persons about whom we gather data through NSLs. The system will also require that specific data elements be entered before the process can continue, such as requiring that the target's status as a United States Person or non-United States Person be entered. The system will not permit requests containing logically inconsistent answers to proceed.

The NSL system is being designed so that the FBI employee requesting an NSL will enter data only once. For example, an agent or analyst who wishes to get telephone toll billing records will only have to prompt the system that he is seeking an ECPA NSL for toll records and type the telephone number once. The system will then automatically populate the appropriate fields in the NSL and the authorizing EC. The system will then generate both the NSL and the authorizing EC for signature, thereby ensuring that the two documents match exactly and minimizing the opportunity for transcription errors that give rise to unauthorized collections that must be reported to the Intelligence Oversight Board (IOB). Agents and analysts will still be required to provide the narrative necessary to explain why the NSL is being sought, the factual basis for making a determination that the information is relevant to an appropriately predicated national security investigation, and the factual basis for a determination whether the NSL should include a non-disclosure provision. In addition, this system will have a comprehensive reporting capability.

We began working with developers on the NSL system in February 2006 and we are optimistic that we will be able to pilot it this summer and roll it out to all field offices by the end of

the year. At that point, I will be confident the data we provide to Congress in future reports is as accurate as humanly possible.

In the meantime, we are taking several steps to correct the numbers we have previously reported. First, we are making data corrections in our database. Through a computer program, we have identified all entries that must be erroneous because there is an apparent error in the entry (e.g., there are more NSLs reported than requests; the date shows a year that is impossible (203)). We are manually reviewing those entries and making corrections. We have also started a random sampling of ten percent of the total entries in the OGC database which contains approximately 64,000 entries. Those entries will be manually checked against ACS. We will determine whether there is a significant difference between the entries in our database and the actual information in ACS. To the extent there is a difference, that will be the factor that will be used to correct our prior reporting. While not yielding an exact count, we believe that to be a statistically appropriate way of correcting prior reporting. We have discussed this methodology with the OIG and will offer it the opportunity to review our work. We are striving to have corrected reports to Congress as soon as possible.

As with the other shortcomings identified by the OIG, there was no finding of an intent to deceive Congress concerning our use of NSLs. In fact, as noted, we identified deficiencies in our system for generating data prior to the initiation of the OIG's review and flagged the issue for Congress almost one year ago. While we do not know the extent of the inaccuracies in past reporting, we are confident that the numbers will not change by an order of magnitude.

Exigent Letters

The next significant finding of the OIG involved the use within one unit at Headquarters of so-called "exigent letters." These letters, which numbered in excess of 700, were provided to

telephone companies with requests for toll billing information regarding telephone numbers. All of the letters stated that there were exigent circumstances. Many of the letters stated that federal grand jury subpoenas had been requested for the records even though in fact no such request for grand jury subpoenas had been made, while others promised future national security letters. From an audit and internal control perspective, the FBI did not document the nature of the emergency circumstances that led it to ask for toll records in advance of proper legal process, did not keep copies of all of the exigent letters it provided to the telephone companies, and did not keep records showing that it had subsequently provided either the legal process promised or any other legal process. Further, based on interviews the OIG conducted, some employees indicated that there was not always any emergency relating to the documents that were sought.

OGC has been working with the affected unit to attempt to reconcile the documentation and to ensure that any telephone record we have in an FBI database was obtained because it was relevant to an authorized investigation and that appropriate legal process has now been provided. As of late last week, there were still a small handful of telephone numbers that had not been satisfactorily tied to an authorized investigation. If we are unable to determine the investigation to which those telephone numbers relate, they will be removed from our database and destroyed.

The OIG rightfully objected to the FBI obtaining telephone records by providing a telephone carrier with a letter that states that a federal grand jury subpoena had been requested when that was untrue. It is unclear at this point why that happened. The Director has ordered a special inspection in order to better understand the full scope of internal control lapses.

We also concur with the OIG that it is inappropriate to obtain records on the basis of a purported emergency if, in fact, there is no emergency. We continue to believe, however, that providers had

the right to rely on our representation that there was an emergency and that the "exigent letters" - had they been issued only when there was an exigent circumstance and had they correctly identified the legal process that would follow - would have been an appropriate tool to use.

In response to the obvious internal control lapses this situation highlights, changes have already been made to ensure that this situation does not recur. Any agent who needs to obtain ECPA-protected records on an emergency basis must now do so pursuant to 18 U.S.C. 2702. Section 2702(c)(4) permits a carrier to provide information regarding its customers to the government 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 of information relating to the emergency. A request for disclosure pursuant to that statute generally must be in writing and must clearly state that the disclosure without legal process is at the provider's option. The letter request must also set out the basic facts of the emergency so that the provider can make some assessment whether it concurs that there is an emergency.

Intelligence Oversight Board Process

The OIG also examined misuse of NSLs that had been reported (and some that had not been reported) as part of the IOB process. As this committee knows, pursuant to Executive Order 12863 the President has an Intelligence Oversight Board that receives from the agencies in the intelligence community reports of intelligence activities that the agency believes may have been unlawful or contrary to Executive Order or Presidential Directive. This language is interpreted by the FBI and DOJ to mandate the reporting of any violation of a provision of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection if such provision is designed to ensure the protection of individual rights.

The FBI requires its employees to report any violations of law or policy about which they are aware. We encourage employees to err on the side of reporting so that we can be sure that all violations are appropriately reported. In terms of process, all potential violations (called PIOBs - or potential intelligence oversight board violations) are reported to OGC. Lawyers within OGC are responsible for "adjudicating" the violation - that is, determining whether the PIOB is an actual Intelligence Oversight Board violation. If it is, a report is made to the IOB, a copy is provided to DOJ and a copy is provided to the FBI's Inspection Division. If the violation involved intentional misconduct, the Inspection Division will determine whether the matter should be referred to the Office of Professional Responsibility for discipline.

The OIG found that from 2003 through 2005, the FBI had self-reported 26 potential violations involving NSL authorities. Of the 26, OGC adjudicated 19 to be violations and reported them. The OIG agreed with each of those determinations. Of the 7 PIOBs that OGC determined were not violations, the OIG agreed with all but one. As to the one determination about which we disagreed, upon re-review, the FBI concurred with the OIG that it was a violation that should have been reported and it has since been reported to the IOB. These 20 violations included: third party errors (4), NSLs issued when the authority for the investigation had lapsed (3), obtaining ECPA-protected records without any legal process (3) and obtaining a full credit report in a counterintelligence case (1).

The OIG also found, however, a number of potential IOBs in the files it examined that had not been reported to OGC for adjudication. Although press accounts of the reports have implied that the OIG found massive abuses of the NSL authorities by the FBI, a careful read of the report reflects a different set of facts. The OIG examined 293 NSLs - a reasonably small sample. The sample was

a judgmental sample and the size was chosen because the audit was extremely labor intensive. We do not suggest that the sample was not a fair sample (although it was not random), but only that it is questionable from a statistical standpoint to attempt to extrapolate from a very small sample to an entire population. Moreover, there was wide variation in the number of purported unreported violations from different field offices. The OIG found 8 potential violations that were unreported in files in both the Philadelphia and Chicago field offices, but only 2 unreported potential violations from files in New York and 4 from San Francisco. We are doing additional follow-up work, but the wide variance between field offices may be a function of the very small sample, or it may indicate that the percentages of potential errors detected are not constant across all field offices.

Setting aside questions about whether the sample is representative, I urge you to look closely at the numbers before arriving at the conclusion that there is a systemic problem concerning the use of NSLs. Of the 293 NSLs the OIG examined, 22 (7%) were judged to have potential unreported IOB violations associated with them. Moreover, of that 7%, 10 - or almost 50% - were third party errors -- that is, the NSL recipient provided the FBI information we did not seek. Only 12 of the NSLs examined - 4% - had mistakes that the OIG rightfully attributes to the FBI.

Examining the 12 potential errors that were rightfully attributed to the FBI reveals a continuum of seriousness relative to the potential impact on individual rights. Four (or just over 1% of the sample) were serious violations. Specifically, two of the violations involved obtaining full credit reports in counterintelligence investigations (which is not statutorily authorized), one involved issuing an NSL when authorization for the investigation to which it related had lapsed, and one involved issuing an NSL for information that was arguably content, and therefore not available pursuant to an NSL. (In the latter case, the ISP on which the NSL was served declined to produce

the requested material so there was, in fact, no collection of information to which we were not entitled.) The balance of the 12 potential violations identified by the OIG do not, in our view, rise to the same level of seriousness as those 4. The remaining 8 involve errors that are best characterized as arising from a lack of attention to detail, and did not result in the FBI seeking or obtaining any information to which it was not entitled. Those 8 potential violations involved errors such as using the wrong certification language in an NSL (although the appropriate certification is not materially different) and having the NSL and the EC seeking the NSL not entirely consistent. We do not excuse such lack of attention to detail, but we do not believe that such mistakes result in or cause a risk to civil liberties.

In short, approximately 1% of the NSLs examined by the OIG had significant errors that were attributable to FBI actions and that had not been, but should have been, reported as PIOBs.

While a 1% error rate is not huge, it is unacceptable, and we have taken steps to reduce that error rate. First, we are very concerned that of all the potential IOBs involving mistakes in NSLs attributable to the FBI (whether previously reported or not), 3 involved the same mistake: namely, issuing an NSL for a full credit report in a counterintelligence investigation. In order to ensure that this particular error is fully rectified, the FBI ordered all field offices to examine all counterintelligence files in which Fair Credit Report NSLs have been issued since January 1, 2002 in order to ascertain whether the file contains a full credit report. If it does, the credit report must be removed from the file, sequestered with the field office's attorney, and a PIOB must be reported to OGC. The results from that search are due to headquarters by April 16, 2007.

Several other steps we have taken will, we believe reduce the likelihood that the FBI will commit the other mistakes in the future. First, as indicated previously, the FBI is developing an

automated system to prepare NSLs and their authorizing ECs. That system will reduce to zero mistakes such as having the wrong certification language or inconsistency between the NSL and the EC. It will also ensure that the investigative file out of which the NSL is being issued is open. Finally, it will ensure that an NSL for a full credit report cannot be issued out of a counterintelligence file.

Other changes to FBI policy have been made that we believe will facilitate better handling of IOBs and also reduce errors that lead to IOBs. First, last fall we provided comprehensive advice to the field regarding its responsibility towards information obtained as a result of third party errors. That guidance requires all such information to be sequestered and reported to OGC as a PIOB. If the "over collected" information is irrelevant to the investigation (e.g., the telephone company transposed a number and provided us records on the wrong telephone account), then it will be destroyed or returned. No such information should be entered into FBI databases. If the information is relevant to the investigation but simply not within the four corners of the NSL, then the information must be sequestered until a new NSL has been issued for the extra data. After the new NSL has been issued, the information can be entered into FBI databases.

Secondly, we have collected all the rules and policies on NSLs into one document which will be disseminated to the field. Those rules now mandate that, until the deployment of the automated NSL system, all NSLs and ECs be prepared from the exemplars that are provided on OGC's website. That should eliminate many of the mistakes identified by the OIG.

All of these rules will, of course, only reduce or eliminate errors if they are followed. The OIG's report has highlighted for us that there must be some sort of auditing function - above and beyond the IOB process - to systematically ensure that these rules, as well as others that govern our

activities in national security investigations are followed. The FBI has historically been very good at establishing policy and setting rules, but we have not been as proactive as we should have been in establishing internal controls and auditing functions.

The full parameters of the compliance program have not been set, although these aspects have been: the Inspection Division with participation of DOJ's National Security Division and Privacy and Civil Liberties Office is in the process of a special inspection of NSL usage in all 56 field offices and headquarters. That inspection should uncover any other significant problems with our use of this tool but should also tell us whether there are variances between offices in terms of the numbers and types of errors. The results of the inspection will then inform the program that the Attorney General announced of having teams of DOJ lawyers, FBI lawyers and the Inspection Division periodically audit field offices' use of NSLs. That process will begin in April and should result in at least 15 offices being audited this year. We are also considering other proactive compliance programs in order to develop a program that ensures, to the maximum extent possible, that the rules and policies designed to protect privacy and civil liberties are faithfully adhered to by all of our employees, that we promptly identify and correct any violations of law or policy, and that any information collected erroneously is removed from FBI databases and destroyed. In addition, a working group co-chaired by the Office of the Director of National Intelligence and the CPCLO has been convened to examine how NSL-derived information is used and retained by the FBI. The FBI and DOJ's National Security Division will have a representative on this working group. We welcome the Committee's input as we move forward on these initiatives.

The FBI is acutely aware that the only way that we can achieve our mission of keeping the country safe is if we are trusted by all segments of the American public. With events like the

London terror attacks of 2 years ago and the Canadian plot to use fertilizer bombs to destroy buildings in Canada in 2006, we have all become worried about the risk of a catastrophic attack from home grown terrorists. Our single best defense against such an attack is the eyes and ears of all Americans -- but particularly of those segments of the population in which the risk of radicalization is at its highest. We need people in those communities to call us when they hear or see something that looks amiss. We know that we reduce the probability of that call immeasurably if we lose the confidence of those segments of the population. That is one of the reasons that we are looking for ways to assure all Americans that we are respectful of individual rights, including privacy rights, and that we use the tools that have been provided to us consistent with the rules set out by Congress.

I appreciate the opportunity to appear before the Committee and look forward to answering your questions. Thank you.