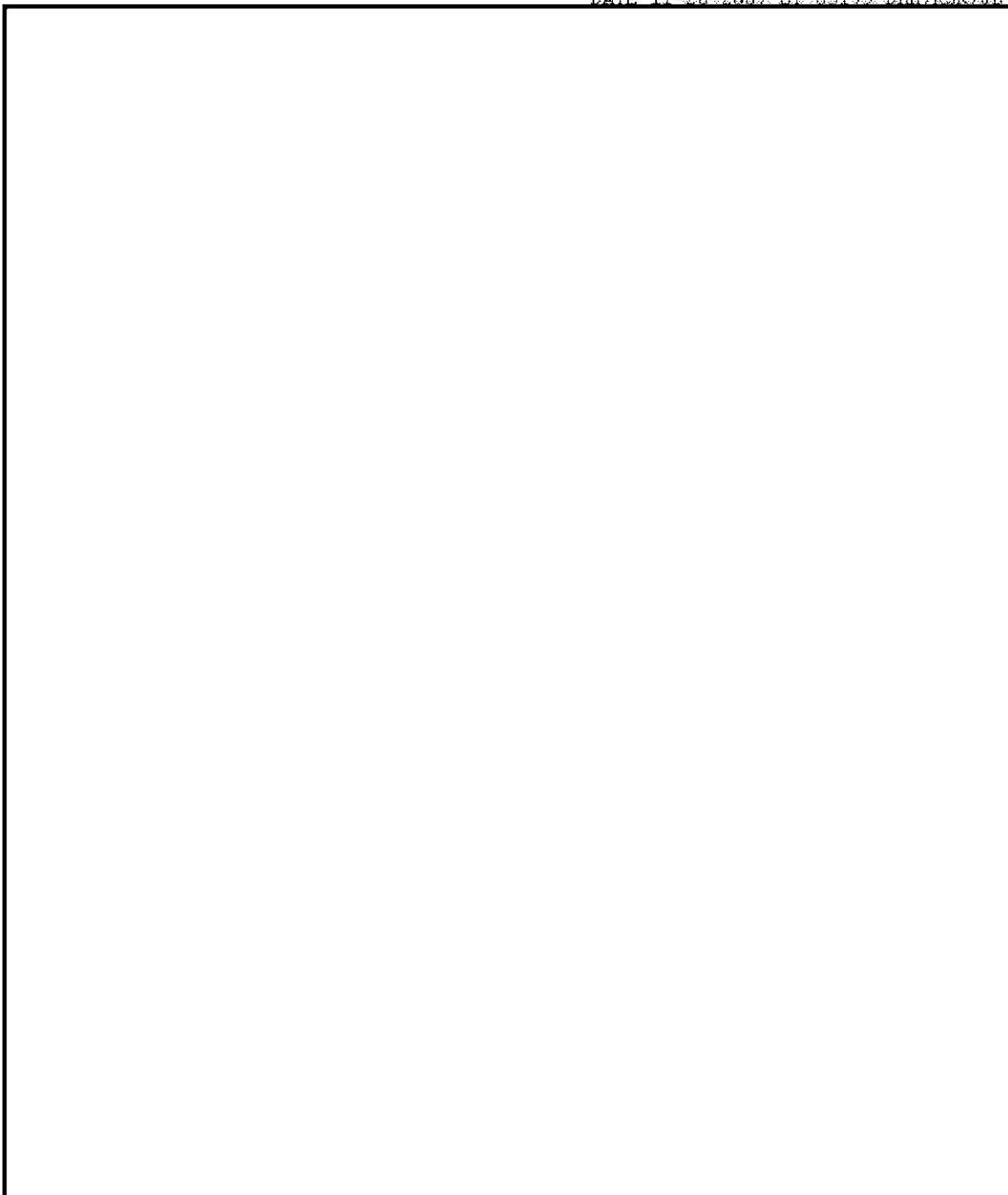


**ECPA NSL Definitions Proposal**

**Section 1. Counterintelligence and counterterrorism access to electronic communication service and remote computing service records.**

Section 2709 of Title 18 is amended

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-20-2007 BY 65179 DMH/KSR/JE



b5

(e)

(f)

(g)

b5

**Section 2. Technical and Conforming Changes**

(a)

## **Analysis**

### **Section 1. Counterintelligence and counterterrorism access to electronic communications service and remote communications service records**

This proposed revision clarifies the scope of the Electronic Communications Privacy Act's national security letter provision, 18 U.S.C. § 2709, by specifically listing the types of records and information that the FBI may obtain pursuant to an ECPA national security letter (NSL).

The list of items contained in this proposal parallels that in 18 U.S.C. § 2703(c)(2) – which identifies the records and information that may be obtained by administrative or grand jury subpoenas – with one exception. In addition to the records and information that may be obtained under section 2703(c)(2), the proposed revision would permit the FBI to obtain “records identifying the origin, routing or destination of electronic communications” using an ECPA NSL. This change would not expand the categories of records and information that may be obtained by an ECPA NSL, but rather would clarify what records or information are obtainable – a change that was suggested by the Department of Justice's Inspector General in his recent report on the use of NSLs by the FBI.

The proposed revision also clarifies the types of providers covered by the ECPA NSL statute by using the language of § 2703(c)(1) to indicate that providers of electronic communication services (which, under the definition contained in § 2510(15), also includes providers of wire communications services) and remote computing services are covered by this provision.

### **Section 2. Technical and Conforming Changes**

The proposed revision changes the table of sections for chapter 121 of title 18 of the United States Code to account for the new title of section 2709.

2Untitled.txt

MessageFrom: [redacted] (OGC) (FBI)  
Sent: Tuesday, August 30, 2005 3:44 PM  
To: [redacted] (OGC) (FBI); [redacted] (CTD) (FBI)

b6  
b7C

SENSITIVE BUT UNCLASSIFIED  
NON-RECORD

[redacted]

Assistant General Counsel b6  
National Security Law Branch b7C  
Office of General Counsel FBI b2  
202-324 [redacted] Voice  
[redacted] Pager  
202-324 [redacted] Secure Fax  
202-324 [redacted] Fax

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-20-2007 BY 65179 DMH/KSR/JB

UNCLASSIFIED

**REPORTING REQUIREMENTS UNDER**

**THE USA PATRIOT IMPROVEMENT and REAUTHORIZATION ACT of  
2005 (Public Law 109-177).**

**&**

**THE USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006  
(Public Law 109-178).**

**FISA BUSINESS RECORD CHANGES**

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

Reporting Cycle:	Attorney General will report on an annual basis (April of each year).
Congressional Committees:	<ul style="list-style-type: none"><li>•House Permanent Select Committee on Intelligence</li><li>•House Judiciary Committee</li><li>•Senate Select Committee on Intelligence</li><li>•Senate Judiciary Committee</li></ul>
Reporting Categories:	<p>(1) Total number of applications for FISA Business Records.</p> <p>(2) Total number of orders granted, modified, or denied.</p> <p>(3) Total number of orders granted, modified, or denied for the special categories of tangible things.</p> <ul style="list-style-type: none"><li>• Library circulation records, library patron lists, book sales records, or book customer lists.</li><li>• Firearms sales records.</li><li>• Tax return records.</li><li>• Educational records.</li><li>• Medical records containing information that would identify a person.</li></ul>
Additional unclassified report:	Annually (April of each year), the Attorney General shall make an unclassified report on the total number of FISA Business Records applications, and the total number of orders granted, modified, or denied.

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-20-2007 BY 65179 DMH/ESR/JB

UNCLASSIFIED

1

NSL VIO-34734

UNCLASSIFIED

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

<p>Scope of Audit:</p>	<p>The IG will perform a comprehensive audit of the effectiveness and use, including any improper or illegal use, of the investigative authority.</p>
<p>Timing of Audit:</p>	<p>For 2002, 2003, and 2004, the audit should be completed within one year of enactment (March 9, 2007).</p> <p>For 2005 and 2006, the audit should be completed by December 31, 2007.</p>
<p>Report results to Congress:</p>	<p>The IG shall submit the audit reports to –</p> <ul style="list-style-type: none"> <li>• House Judiciary Committee.</li> <li>• House Permanent Select Committee on Intelligence.</li> <li>• Senate Judiciary Committee.</li> <li>• Senate Select Committee on Intelligence.</li> </ul>
<p>Examine effectiveness of the tool:</p>	<p>Audit will look at the following for effectiveness –</p> <ul style="list-style-type: none"> <li>• Categories of records obtained.</li> <li>• The importance to the FBI and the IC of the information obtained.</li> <li>• The manner in which the information is collected, retained, analyzed, and disseminated by the FBI (this will include an examination of the access to “raw data” provided by the FBI to other agencies of the Federal, State, local, or tribal governments, or private sector agencies).</li> <li>• The minimization procedures adopted by the AG.</li> <li>• Whether, and how often, the FBI used information to produce analytical intelligence products for the FBI, the IC, or other Federal, State, local, or tribal government agencies.</li> <li>• Whether, and how often, the FBI provided the information to law enforcement authorities for criminal proceedings.</li> </ul>

UNCLASSIFIED

<b>Examine the process:</b>	The audit process will look at the following: <ul style="list-style-type: none"><li>• How often the FBI requested DOJ to submit an application and the request was not submitted to the court (including the basis for the decision).</li><li>• Whether the court granted, modified, or denied the application.</li><li>• The justification for the failure of the AG to issue implementing procedures governing the requests in a timely fashion, including whether the delay harmed national security.</li><li>• Whether bureaucratic or procedural impediments prevent the FBI from fully using the authority.</li></ul>
-----------------------------	---

**FISA ROVING SURVEILLANCE CHANGES**

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

<b>Reporting cycle:</b>	The Attorney General will report on a semi-annual basis.
<b>Congressional Committees:</b>	<ul style="list-style-type: none"><li>• House Permanent Select Committee on Intelligence</li><li>• Senate Select Committee on Intelligence</li><li>• Senate Judiciary Committee</li></ul>
<b>Reporting categories:</b>	<ul style="list-style-type: none"><li>• Total number of applications made for orders and extensions.</li><li>• Each criminal case in which information has been authorized for use at trial, during the period covered by such report.</li><li>• Total number of emergency employments and total number of subsequent orders approving or denying surveillance.</li></ul>

**FISA OVERSIGHT CHANGES**

Congressional Reporting on FISA Physical Search authority:

<b>Reporting cycle:</b>	Attorney General will report on a semiannual basis.
<b>Congressional Committees:</b>	<ul style="list-style-type: none"><li>• House Permanent Select Committee on Intelligence</li><li>• House Judiciary Committee</li><li>• Senate Select Committee on Intelligence</li><li>• Senate Judiciary Committee</li></ul>

UNCLASSIFIED

Reporting categories:	Report the following regarding emergency physical searches – <ul style="list-style-type: none"> <li>• Total number of applications.</li> <li>• Total number of orders granted, modified, or denied.</li> <li>• Number of physical searches involving the residences, offices, or personal property of U.S. persons, and the number of occasions the AG provided notice.</li> <li>• Total number of emergency authorizations, and total number of subsequent orders approving or denying the physical searches.</li> </ul>
-----------------------	---

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

Reporting cycle:	Attorney General will report on a semiannual basis.
Congressional Committees:	<ul style="list-style-type: none"> <li>• House Permanent Select Committee on Intelligence</li> <li>• House Judiciary Committee</li> <li>• Senate Select Committee on Intelligence</li> <li>• Senate Judiciary Committee</li> </ul>
Reporting categories:	Report the following regarding pen registers/trap and trace – <ul style="list-style-type: none"> <li>• Total number of applications.</li> <li>• Total number of orders granted, modified, or denied.</li> <li>• Total number of emergency authorizations, and total number subsequent orders approving or denying the pen registers/trap and trace.</li> </ul>

**FISA PEN REGISTER/TRAP AND TRACE CHANGES**

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

Reporting cycle:	Attorney General shall report on a semiannual basis.
Congressional Committees:	<ul style="list-style-type: none"> <li>• House Permanent Select Committee on Intelligence</li> <li>• House Judiciary Committee</li> <li>• Senate Select Committee on Intelligence</li> <li>• Senate Judiciary Committee</li> </ul>
Reporting categories:	Use of pen registers and trap and trace.



UNCLASSIFIED

**EMERGENCY DISCLOSURES**

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

Voluntary disclosure by provider:	If the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay.
Reporting cycle:	Attorney General shall report on an annual basis.
Congressional Committees:	<ul style="list-style-type: none"><li>• House Judiciary Committee</li><li>• Senate Judiciary Committee</li></ul>
Reporting categories:	<ul style="list-style-type: none"><li>• Number of accounts from which voluntary disclosures were received.</li><li>• Summary of the basis for disclosure where the investigation was closed without criminal charges.</li></ul>

**NATIONAL SECURITY LETTERS**

**Sec. 118. Reports on National Security Letters.**

Current NSL Reports:	<ul style="list-style-type: none"><li>• AG reports on a semi-annual basis.</li></ul>
	<ul style="list-style-type: none"><li>• Reports will now also be made to the House Judiciary Committee, the House Permanent Select Committee on Intelligence, the Senate Judiciary Committee, and the Senate Select Committee on Intelligence.</li></ul>

Enhanced Oversight of 15 U.S.C. § 1681v NSLs (for credit agency consumer records):	<ul style="list-style-type: none"><li>• AG reports on a semi-annual basis.</li></ul>
	<ul style="list-style-type: none"><li>• Reports will now also be made to the House Judiciary Committee, the House Committee on Financial Services, the House Permanent Select Committee on Intelligence, the Senate Judiciary Committee, the Senate Housing and Urban Affairs Committee, and the Senate Select Committee on Intelligence.</li></ul>

Aggregate Report of NSL requests:	<ul style="list-style-type: none"><li>• AG reports annually (April).</li></ul>
-----------------------------------	--

UNCLASSIFIED

	<ul style="list-style-type: none"> <li>• Total number of NSL (excluding NSLs for subscriber information) requests for information concerning <u>different</u> U.S. persons.</li> </ul>
	<ul style="list-style-type: none"> <li>• Unclassified report.</li> </ul>

**Sec. 119. Enhanced Oversight of National Security Letters.**

<p>Requirements of DOJ IG Audit:</p>	<p>Comprehensive audit of --</p> <ul style="list-style-type: none"> <li>• Use of NSLs for 2003 through 2006.</li> <li>• Description of noteworthy facts/circumstances, including any improper or illegal use of NSLs.</li> </ul>
<p>Timing of Audit:</p>	<ul style="list-style-type: none"> <li>• For 2003 and 2004, must be completed not later than one year after enactment (March 9, 2007).</li> <li>• For 2005 and 2006, must be completed not later than December 31, 2007.</li> </ul>
<p>Examine Effectiveness of NSLs:</p>	<p>The audit will examine:</p> <ul style="list-style-type: none"> <li>• Importance of the information acquired by DOJ to the intelligence activities of DOJ and other members of the IC.</li> <li>• How information is collected, retained, analyzed, and disseminated (including access to raw data) to members of the IC community, and other Federal, State, local or tribal governments, or private sector entities.</li> <li>• How often NSL information was used to produce an analytical intelligence product for distribution to the IC community, and to other Federal, State, local or tribal governments.</li> <li>• Whether, and how often, NSL information was provided to law enforcement authorities for use in criminal investigations.</li> <li>• Following enactment of the USA PATRIOT IRA, the number of NSLs issued without the certification necessary to create a nondisclosure obligation.</li> <li>• Types of electronic communications and transactional information obtained under § 2709, and the procedures DOJ used if content information is obtained.</li> </ul>
<p>Feasibility of Minimization Procedures:</p>	<ul style="list-style-type: none"> <li>• Not later than February 1, 2007, or upon completion of the 2003/2004 audit, the Attorney General and the Director of National Intelligence shall jointly submit a report on the feasibility of applying minimization procedures to protect the constitutional rights of U.S. persons.</li> </ul>

UNCLASSIFIED

	<ul style="list-style-type: none"><li>• Report goes to the House Judiciary Committee, the House Permanent Select Committee on Intelligence, the Senate Judiciary Committee, and the Senate Select Committee on Intelligence.</li></ul>
--	--

**DELAYED NOTICE SEARCH WARRANTS**

**Sec. 114. Delayed Notice Search Warrants.**

Reporting	Annual reporting to Congress by Court (starting with the fiscal year ending September 30, 2007).
-----------	--

**DATA-MINING ACTIVITIES**

**Sec. 126. Report on Data-Mining Activities.**

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

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

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



FEDERAL BUREAU OF INVESTIGATION

**Precedence:** PRIORITY

**Date:** 10/02/2006

**To:** All Field Offices

**Attn:** ADIC  
SAC  
CDC

All Legats  
Counterterrorism  
Criminal Investigative  
Cyber  
Counterintelligence

**Attn:** Legats  
**Attn:** A/AD Joseph Billy, Jr.  
**Attn:** AD James H. Burrus  
**Attn:** AD James E. Finch  
**Attn:** AD Timothy D. Berezney

**From:** Office of the General Counsel  
Investigative Law Unit

**Contact:** SSA [redacted] (202) 324-[redacted]

**Approved By:** Caproni Valerie E  
Lammert Elaine N  
Thomas Julie F

b2  
b6  
b7C

[redacted]

**Drafted By:**

**Case ID #:** 66F-HQ-1085159 (Pending)  
66F-HQ-1085165 (Pending)

**Title:** NEW ANNUAL REPORTING REQUIREMENT  
EMERGENCY DISCLOSURES UNDER 18 U.S.C. 2702 (b)(8)

**Synopsis:** To advise FBI Headquarters Divisions and Field Offices of the annual reporting requirement regarding voluntary disclosures made by service providers to the FBI pursuant to the emergency disclosure provision of Title 18, United States Code, Section 2702 (b)(8), and to set forth procedures for facilitating the same.

**Enclosure(s):** Enclosed is a copy of a memorandum from the Department of Justice (DOJ), dated July 10, 2006, and entitled "Reporting Requirement Under Section 107 of the USA PATRIOT Improvement and Reauthorization Act of 2005."

**Details:** On March 9, 2006, the USA PATRIOT Improvement and Reauthorization Act of 2005, (USA PATRIOT IRA), was signed into law. The USA PATRIOT IRA made several changes to various criminal laws, including 18 U.S.C. § 2702(b)(8) which permits an electronic communications service provider to voluntarily disclose to law enforcement the content of customer communications if the provider, "in good faith, believes that an emergency involving danger of death or serious physical injury to

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-20-2007 BY 65179 DMH/KSR/JB

NSL VIO-34742

To: All Field Offices From: Office of the General Counsel  
Re: 66F-HQ-1085159, 10/02/2006

any person requires disclosure without delay of communications relating to the emergency." The emergency disclosure provision can be used in both criminal cases and national security investigations. For further legal guidance on use of the emergency disclosure provision, see the Electronic Communication (EC) from OGC to All Field Offices, dated August 25, 2005, and entitled "Emergency Disclosure Provision for Information from Service Providers under 18 U.S.C. § 2702(b)" (66F-HQ-1085159, Serial 65).

18 U.S.C. 2702(b)(8) was amended to include the following DOJ reporting requirements:

"Section 107. ENHANCED OVERSIGHT OF GOOD-FAITH EMERGENCY DISCLOSURES UNDER SECTION 212 OF THE USA PATRIOT ACT

(a) ENHANCED OVERSIGHT-Section 2702 of title 18, United States Code, is amended by adding at the end the following:

(d) REPORTING OF EMERGENCY DISCLOSURES-On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing-

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and

(2) a summary of the basis for disclosure in those instances where-

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges."

This reporting requirement was intended to allay concerns raised during the USA PATRIOT ACT reauthorization process that the use of the voluntary disclosure provision lacked adequate oversight and that disclosures were being made in situations which were not truly emergency situations.

Receiving offices are reminded that the emergency disclosure provision under 18 U.S.C. 2702 (b)(8) is limited to those situations where the service provider, in good faith, believes that an emergency involving death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency. While the service provider is responsible for determining the amount of information

To: All Field Offices From: Office of the General Counsel  
Re: 66F-HQ-1085159, 10/02/2006

it needs to reach this "good faith" belief, it is possible that they can reach this determination solely based on a statement from the FBI or another entity that such an emergency exists. Agents should seek the advice of their Chief Division Counsel (CDC), the Investigative Law Unit, or the National Security Law Branch, if they have a question regarding whether the facts of a particular case create an emergency situation supporting the use of the emergency disclosure provision.

Emergency disclosures may also be made in regard to the records associated with the communications. However, the reporting requirement is limited to those cases where the content of communications is disclosed.<sup>1</sup>

DOJ will be responsible for reporting the above information to Congress. To ensure consistency in component reporting, DOJ created a single form for all components to utilize to capture and track information relating to this reporting requirement. The form, a sample of which is included as part of the enclosure to this EC, contains the following fields which must be completed for every case where a provider voluntarily discloses content of an electronic communication pursuant to Section 2702(b)(8):

- 1) Date of Disclosure
- 2) Account
- 3) Basis for Disclosure
- 4) Investigation Opened (yes/no)
- 5) Date Investigation Opened
- 6) Case File Number
- 7) Investigation Closed (yes/no)
- 8) Date Investigation Closed
- 9) Criminal Charges Filed (yes/no)
- 10) Charges Filed
- 11) Entity Bringing Charges

For purposes of completing the form, the following guidelines should be followed:

(1) The disclosures should be organized by account. Typically, when the FBI seeks information from an electronic service provider or a remote computing service (usually an ISP) pursuant to Section 2702(b)(8), the FBI informs the provider that the request is directed at a specific account or an online identity,

---

<sup>1</sup>The Act also modified the emergency standard for the disclosure of records to mirror that used for the disclosure of content.

To: All Field Offices From: Office of the General Counsel  
Re: 66F-HQ-1085159, 10/02/2006

such as a screen name. When the ISP provides the information to the FBI, the FBI may receive information that a subscriber has multiple accounts or that an account has multiple identities. These accounts should be reported separately. For example, if an ISP provides information that three e-mail addresses are held by one individual, the FBI will report that it received information on three accounts;

(2) A summary of the basis for the disclosure must be retained. The summary should contain sufficient information to allow an individual unfamiliar with the investigation to assess whether there could have been a good faith belief that an emergency existed;

(3) Disclosures made pursuant to 18 U.S.C. 2702(b)(8) and subsequent investigations must be tracked to determine whether an investigation was closed without the filing of criminal charges;

(4) Although recipients should provide the number of accounts that disclosures were received from within a given year, a summary of the basis for disclosure should not be reported unless and until the investigation is closed without the filing of criminal charges; and

(5) In task force situations where the FBI is the lead agency, it is responsible for making the report. In those task force situations where the FBI is not the lead agency but nevertheless receives the disclosure directly from the ISP, then the FBI should also make a report. If more than one DOJ entity on the task force receives a disclosure directly from the ISP, the FBI should coordinate with those other DOJ task force entities to ensure that only one report is made.

DOJ's first report will cover the period from July 1, 2006 through December 31, 2006. For subsequent years, the reporting period will cover the period from January 1 through December 31. Each field office and FBIHQ Division will be responsible for immediately maintaining the information set forth in the attached form in an appropriate office control file. A separate control file will be necessary for any classified material. In order to avoid duplicate reporting, an entity that submits a request for an emergency disclosure is responsible for recording the information. The forms will be transmitted by the field and FBIHQ Divisions to the Investigative Law Unit (ILU), Office of the General Counsel, on an annual basis. ILU will advise the field offices and FBIHQ Divisions by EC as to the deadline for transmittal each year. The first deadline for transmittal will be January 31, 2007.



To: All Field Offices From: Office of the General Counsel  
Re: 66F-HQ-1085159, 10/02/2006

Each Field Office and FBIHQ Division shall designate a Point of Contact (POC) for compiling the annual report to ILU and shall notify ILU via electronic communication (EC) of that POC on or before **December 8, 2006**. Further, ***all Field Office Squad Supervisors whose Agents receive emergency disclosures subject to this reporting requirement are responsible for providing the requested information to the Field Office POC.***

Finally, it should be noted that all of the information contained in the form will not be transmitted by DOJ to Congress. The form simply provides a uniform method for tracking information so that if later questions are received by the Department relating to the report, there is a mechanism in place to identify the case in which the disclosure was received.

Any questions should be directed to the Investigative Law Unit at (202) 324- or the National Security Law Branch at (202)324-

b2

To: All Field Offices From: Office of the General Counsel  
Re: 66F-HQ-1985159, 10/02/2006

**LEAD(s) :**

**Set Lead 1: (Action)**

ALL RECEIVING OFFICES

Each Field Office and FBIHQ Division shall designate a Point of Contact (POC) for compiling the annual Field Office report to ILU and shall notify ILU via electronic communication (EC) of that POC on or before **December 8, 2006**.

**Set Lead 2: (Action)**

ALL RECEIVING OFFICES

Please distribute to all employees. Each Field Office and FBIHQ Division shall provide the first annual report to the Investigative Law Unit by **January 31, 2007**.

◆◆

Outside the Scope 4/4/07 email

~~SECRET~~



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

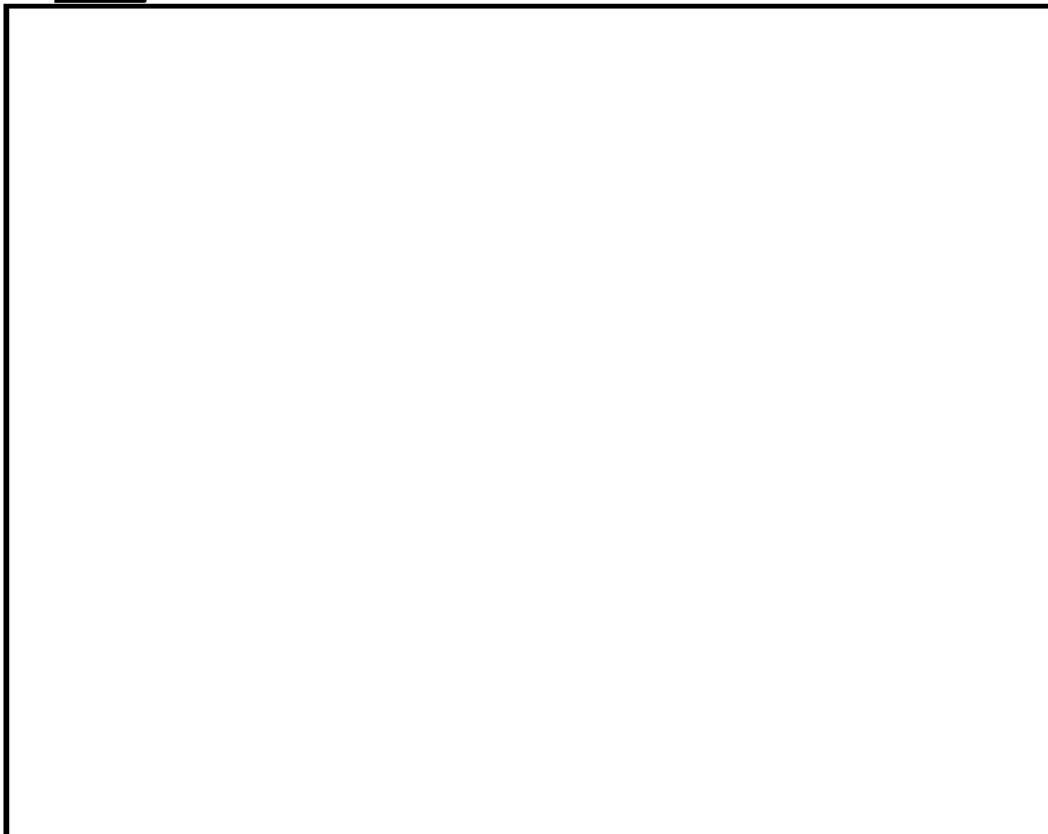
**From:** [redacted] (CTD) (FBI)  
**Sent:** Tuesday, February 27, 2007 9:33 AM  
**Subject:** Additional CAU capabilities

b6  
b7C

(S) ~~SECRET//ORCON.NOFORN~~  
~~RECORD~~ [redacted]

b1

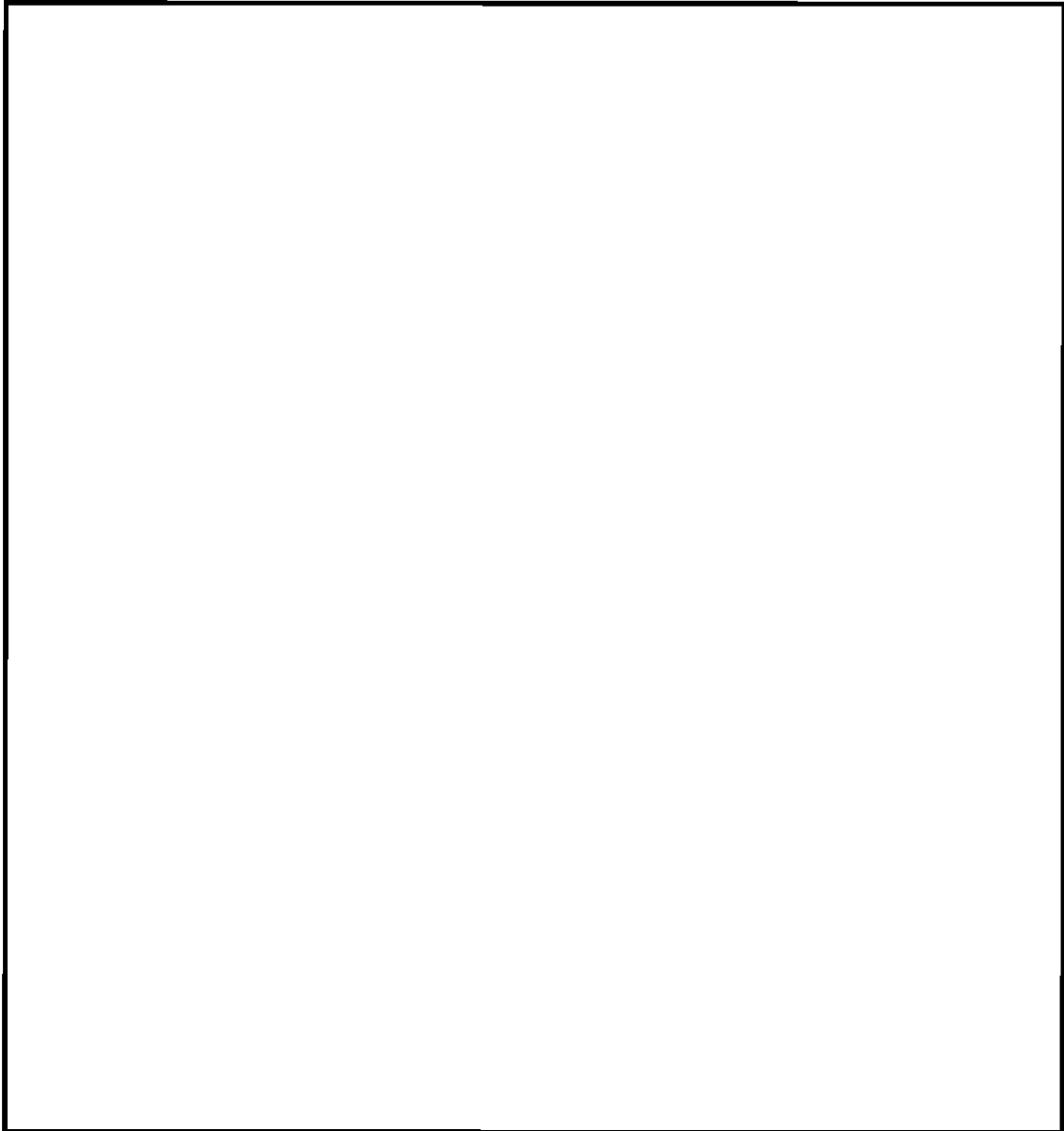
Hi [redacted]



b6  
b7C  
b4  
b7D  
b5  
b2  
b7E

~~SECRET~~ NSL VIO-34792

~~SECRET~~





b5

Good luck on your investigations and let me know if you need anything else. :)



Intelligence Analyst  
CTD / CXS / CAU  
FBIHQ - Room 4512

 binet fbj  
(202) 324-

b7C  
b6  
b2

"Be the change you wish to see in the world..." - Gandhi

~~DERIVED FROM: Multiple Sources~~

~~SECRET~~ VIO-34793

~~SECRET~~

~~DECLASSIFICATION EXEMPTION 1~~  
~~SECRET//ORCON,NOFORN~~

~~DERIVED FROM: Multiple Sources~~  
~~DECLASSIFICATION EXEMPTION 1~~  
~~SECRET//ORCON,NOFORN~~

~~DERIVED FROM: Multiple Sources~~  
~~DECLASSIFICATION EXEMPTION 1~~  
~~SECRET//ORCON,NOFORN~~

~~DERIVED FROM: Multiple Sources~~  
~~DECLASSIFICATION EXEMPTION 1~~  
~~SECRET//ORCON,NOFORN~~

~~DERIVED FROM: Multiple Sources~~  
~~DECLASSIFICATION EXEMPTION 1~~  
~~SECRET//ORCON,NOFORN~~

~~DERIVED FROM: Multiple Sources~~  
~~DECLASSIFICATION EXEMPTION 1~~  
~~SECRET//ORCON,NOFORN~~

~~DERIVED FROM: Multiple Sources~~  
~~DECLASSIFICATION EXEMPTION 1~~  
~~SECRET//ORCON,NOFORN~~

~~DERIVED FROM: Multiple Sources~~  
~~DECLASSIFICATION EXEMPTION 1~~  
~~SECRET//ORCON,NOFORN~~

~~DERIVED FROM: Multiple Sources~~  
~~DECLASSIFICATION EXEMPTION 1~~  
~~SECRET//ORCON,NOFORN~~

~~DERIVED FROM: Multiple Sources~~  
~~DECLASSIFICATION EXEMPTION 1~~  
~~SECRET//ORCON,NOFORN~~

~~DERIVED FROM: Multiple Sources~~  
~~DECLASSIFICATION EXEMPTION 1~~  
~~SECRET//ORCON,NOFORN~~

~~SECRET~~

NSL VIO-34794

From:

[redacted] OGC(FBI)

Sent:

Friday, January 26, 2007 3:14 PM

To:

[redacted] (OGC) (FBI) [redacted] (OGC)  
(FBI)

b6  
b7C

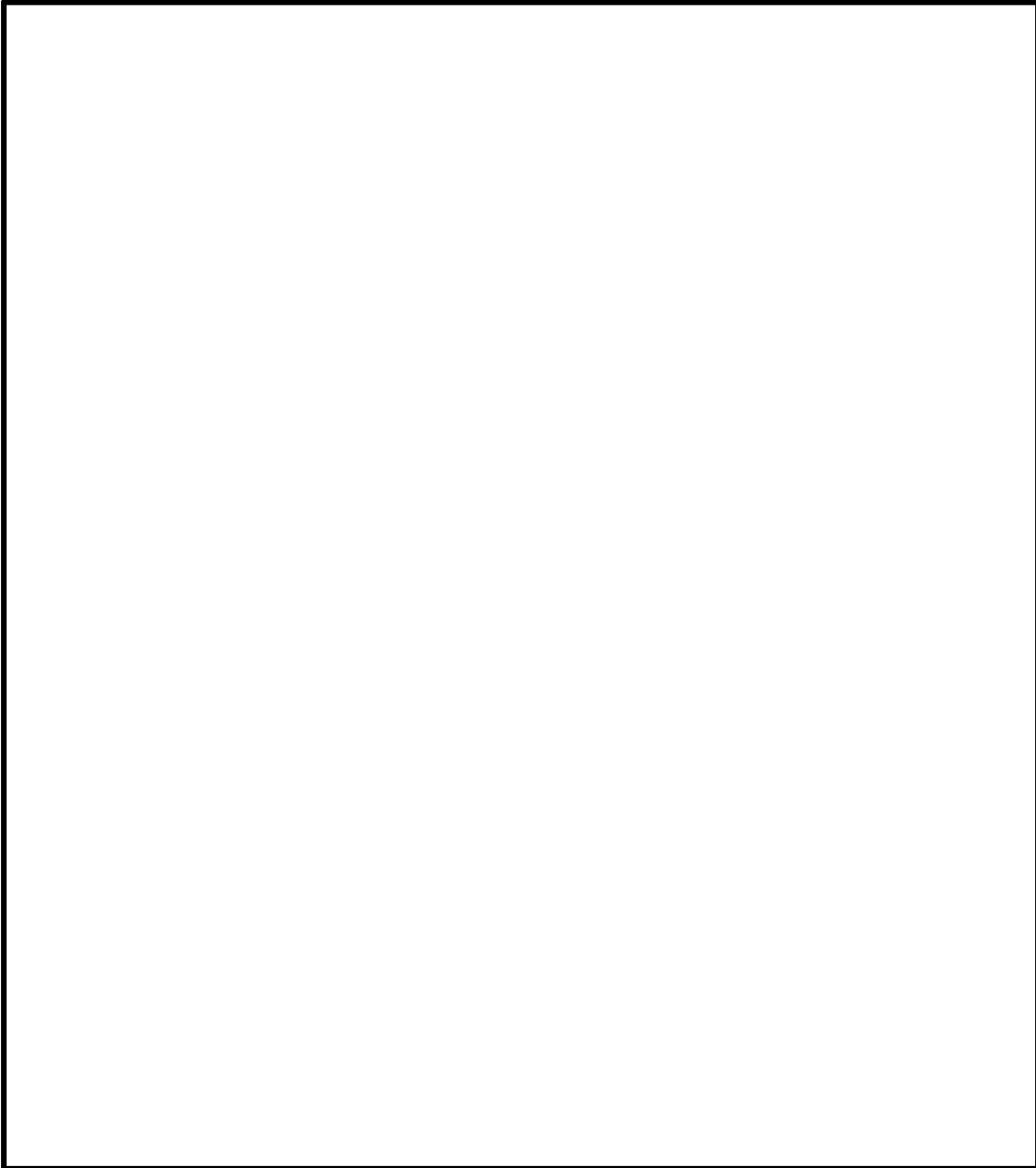
Subject:

RE: NSL for electronic communications provider

~~SECRET~~  
~~RECORD 345N~~

I AM NOT SURE WHO WROTE THIS BUT [redacted]

[redacted] USE OUR PONY ON THE WEB SITE WHICH [redacted] WROTE AND MY  
ADDENDUM



ESR/JE

b5

b6  
b7C  
b2

[Redacted]  
Assistant General Counsel  
National Security Law Branch  
Office of General Counsel FBI  
202-324-[Redacted] Voice  
[Redacted] Pager  
202-324-[Redacted] Secure Fax  
202-324-[Redacted] Fax

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

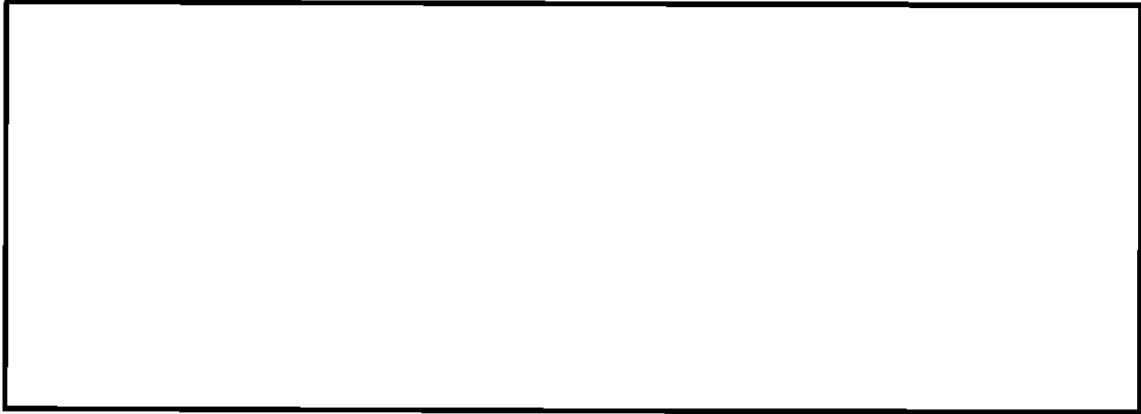
b6  
b7C

**From:** [Redacted] (OGC) (FBI)  
**Sent:** Friday, January 26, 2007 2:55 PM  
**To:** [Redacted] (OGC)(FBI); [Redacted] (OGC) (FBI)  
**Subject:** NSL for electronic communications provider

~~SECRET~~  
Duplicate 1/26/07 email/Email of OGC Employee No. 74

[Redacted]

Duplicate



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

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



**From:** [redacted] (OGC)(FBI)  
**Sent:** Monday, April 10, 2006 5:49 PM  
**To:** [redacted] (OGC) (FBI); [redacted] (OGC) (FBI);  
[redacted] (OGC) (FBI); [redacted] (OGC)  
(FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)  
**Subject:** RE: Website info

b6  
b7C

~~SECRET~~  
**RECORD 197-C841-A2**

[redacted] as I recall wasn't [redacted] has asked this question before [redacted]  
[redacted]

b6  
b7C  
b5  
b2  
b7E

[redacted]  
Assistant General Counsel  
National Security Law Branch  
Office of General Counsel FBI  
202-324-[redacted] Voice  
[redacted] Pager  
202-324-[redacted] Secure Fax  
202-324-[redacted] Fax

b6  
b7C  
b2

DECLASSIFIED BY: 65179 DMH/KSR/JB  
ON: 11-20-2007

-----Original Message-----  
**From:** [redacted] (OGC) (FBI)  
**Sent:** Monday, April 10, 2006 2:05 PM  
**To:** [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC)  
(FBI); [redacted] (OGC)(FBI); [redacted] (OGC) (FBI); [redacted] (OGC)  
(FBI)  
**Subject:** RE: Website info

b6  
b7C

~~SECRET~~  
**RECORD 197-C841-A2**

[redacted]

b5

-----Original Message-----  
**From:** [redacted] (OGC) (FBI)  
**Sent:** Monday, April 10, 2006 1:53 PM  
**To:** [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted]  
(OGC)(FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI);  
[redacted] (OGC) (FBI)  
**Cc:** [redacted] (OGC) (FBI)  
**Subject:** Fw: website info

b6  
b7C

~~SECRET~~  
**RECORD 197-C841-A2**

All  
See the emails below. Here is the issue [redacted]

b5

[Redacted]

My view is [Redacted]

[Redacted]

b5  
b2  
b7E

My recommendation was to submit it as a potential IOB. Once we get the EC, then OGC can decide whether it was an IOB violation. As you can see, the field [Redacted] [Redacted] Please let me know what you think so that I can give a final answer (I might have to run it by Julie first). Thanks for your thoughts in advance.

b6  
b7C

[Redacted]

-----Original Message-----  
**From:** [Redacted] (FBI)  
**Sent:** Friday, March 31, 2006 12:09 PM  
**To:** [Redacted] (OGC) (FBI)  
**Subject:** FW: Website info

b6  
b7C  
b2  
b7E

~~SECRET~~  
**RECORD 197-C841-A2**

[Redacted] I understand that although he originally suggested the issue discussed below was an IOB violation, [Redacted] has now deferred to NSL B on the matter (and you are the lucky atty assigned to it). I sent the below e-mail to [Redacted] to relay the [Redacted] CDC's position on the matter and to request further information [Redacted]

b6  
b7C  
b5  
b2  
b7E

[Redacted]

-----Original Message-----  
**From:** [Redacted] (FBI)  
**Sent:** Friday, March 31, 2006 11:49 AM  
**To:** [Redacted] (FBI)  
**Cc:** [Redacted] (FBI)  
**Subject:** Website info

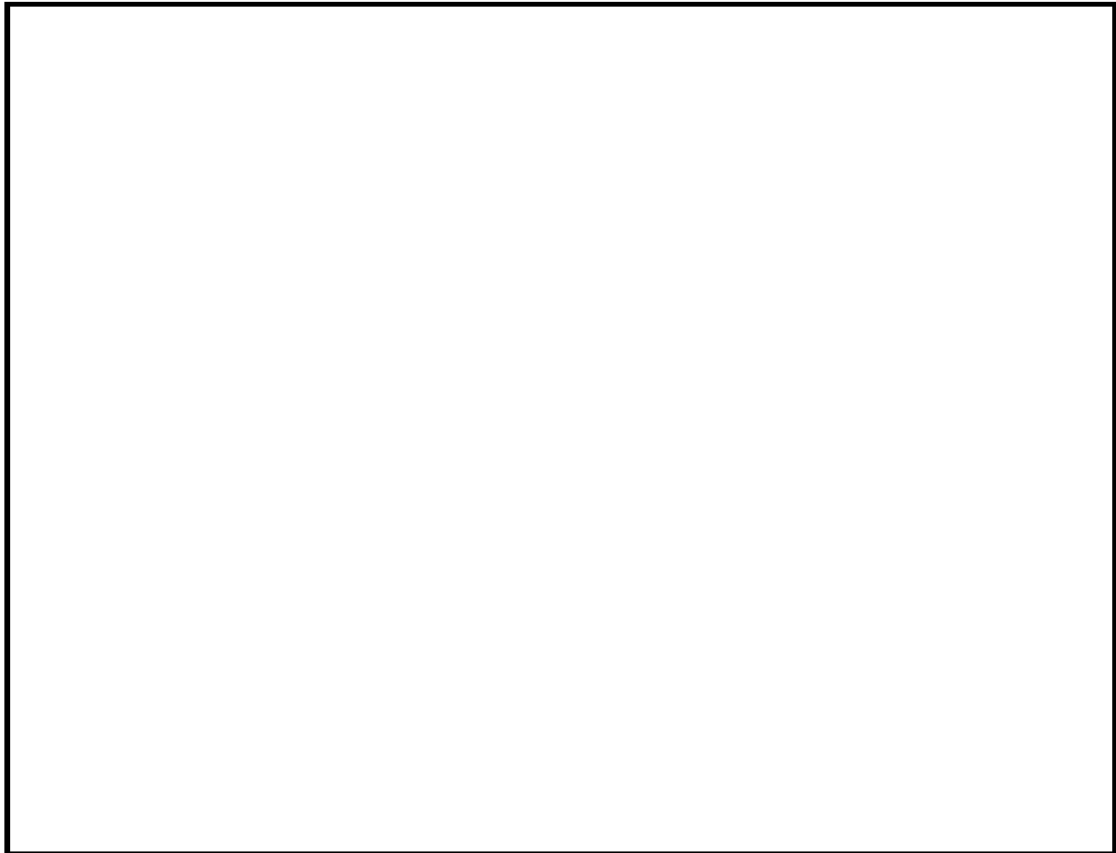
b6  
b7C  
b2  
b7E

~~SECRET~~  
**RECORD 197-C841-A2**

Hi [Redacted] I hope you are doing well. I wanted to let you know that I am the [Redacted] ADC

[Redacted]

b6  
b7C  
b5  
b2  
b7E



b6

Please let me know the status so we can take appropriate action. Thanks.



**\*\*\*\*This Document Contains Attorney Work Product and Attorney-Client Privileged Communications\*\*\*\***

SSA   
Associate Division Counsel



b6  
b7C  
b2  
b7E

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations  
DECLASSIFICATION EXEMPTION 1  
SECRET~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign Counterintelligence Investigations  
DECLASSIFICATION EXEMPTION 1  
SECRET~~

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

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

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



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

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

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

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

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

[NAME, IF KNOWN]

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-20-2007 BY 65179 DMH/KSR/JB

[ADDRESS, IF KNOWN]

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

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

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

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

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

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

NSL VIO-34804

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

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

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

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

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

**[Include the following language in all NSLs.]**

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

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

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

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

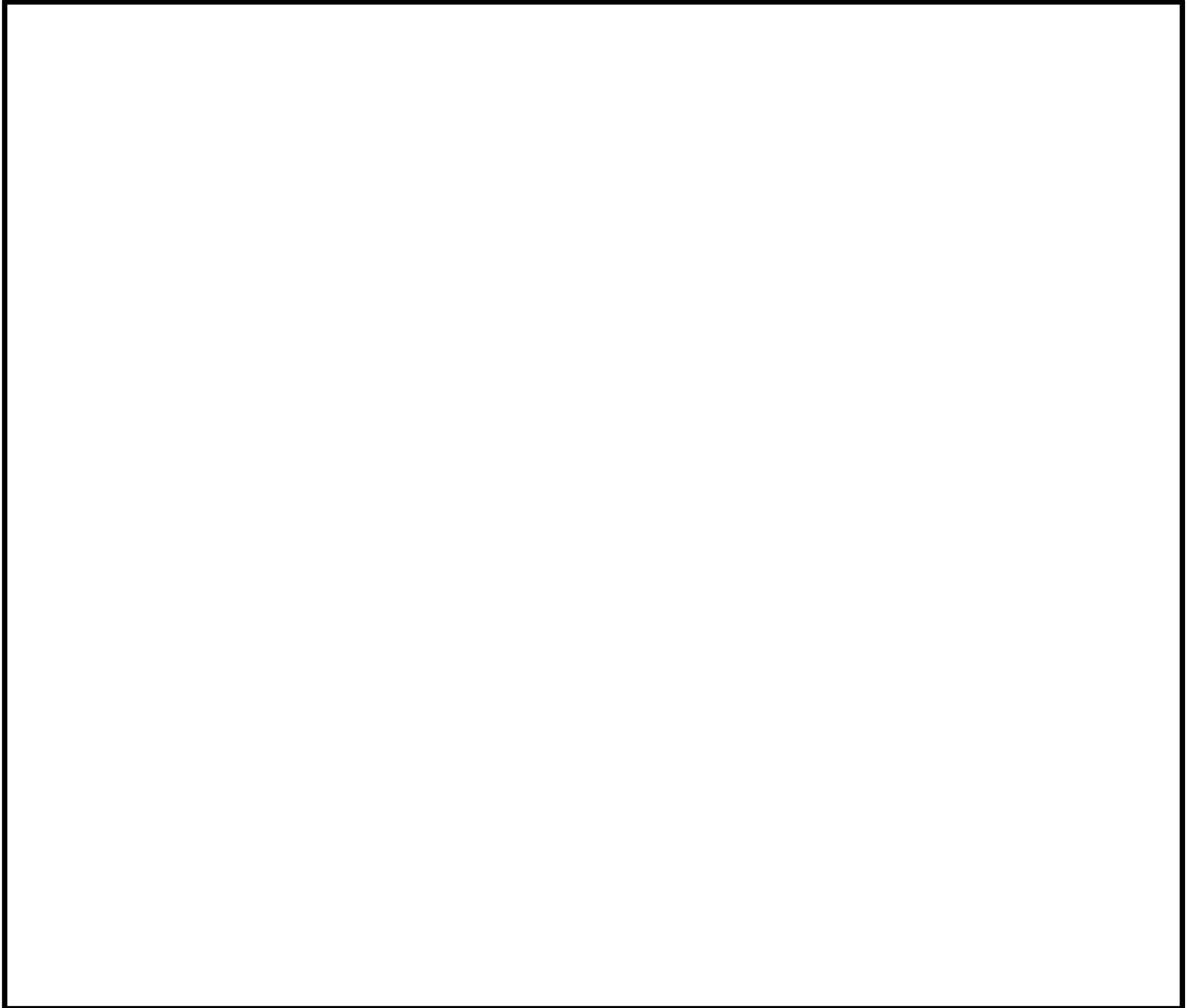
Your cooperation in this matter is greatly appreciated.

Sincerely yours,

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

ATTACHMENT

In preparing your response to this National Security Letter, you should determine whether your company maintains the following types of information which may be considered by you to be toll billing records in accordance with Title 18, United States Code, Section 2709:



We are not requesting, and you should not provide, information pursuant to this request that would disclose the content of any wire communication as "content" is defined in Title 18, United States Code, Section 2510(8).

b2  
b7E



Untitled.txt

MessageFrom: [redacted] (OGC) (FBI)  
Sent: Friday, July 29, 2005 2:26 PM  
To: [redacted] (OGC) (FBI)

b6  
b7C  
b2

UNCLASSIFIED  
NON-RECORD

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-20-2007 BY 65179 DMH/KSR/SE

[redacted]  
Assistant General Counsel  
National Security Law Branch  
Office of General Counsel FBI  
202-324-[redacted] Voice  
[redacted] Pager  
202-324-[redacted] Secure Fax  
202-324-[redacted] Fax

UNCLASSIFIED

UNCLASSIFIED

**USA PATRIOT IMPROVEMENT and REAUTHORIZATION ACT of 2005  
(Public Law 109-177).**

&

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 11-20-2007 BY 65179 DMH/KSR/JB

**USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006  
(Public Law 109-178).**

Chart Summaries of recent changes to national security legal authorities as a result of the "USA PATRIOT Improvement and Reauthorization Act of 2005" and the "USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006."

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

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

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

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

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

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

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

UNCLASSIFIED

1

NSL VIO-34809

UNCLASSIFIED

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

- **Title V - Miscellaneous Provisions**

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

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

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

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

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

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

**SUNSET PROVISIONS**

**Sec. 102. USA PATRIOT Act Sunset Provisions.**

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

- Sections 201 & 202 (Expanded Title III predicates);
- Section 203(b) & (d) (Information sharing for foreign intelligence obtained in Title III and criminal investigations);
- Section 204 (Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral and Electronic Communications);
- Section 207 (Extended duration of certain FISAs);
- Section 209 (Seizure of voice mail with a search warrant);
- Section 212 (Emergency disclosures of e-mail and records by ISPs);
- Section 214 (FISA pen/trap authority);

UNCLASSIFIED

Section 217 (Interception of computer trespasser communications);  
 Section 218 (Change in the probable cause (“significant purpose”) standard of FISA);  
 Section 220 (Nationwide search warrants for electronic evidence);  
 Section 223 (Civil liability for certain unauthorized disclosures); and,  
 Section 225 (Immunity for compliance with FISA wiretap).

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

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

Provision	New Sunset Date
FISA “Lone Wolf”	December 31, 2009

**FISA DURATION CHANGES**

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

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

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

UNCLASSIFIED

**FISA BUSINESS RECORD CHANGES**

**Sec. 106. Access to Certain Business Records Under Section 215 of the USA PATRIOT Act.<sup>1</sup>**

<p>Scope of FISA Business Records authority:</p>	<ul style="list-style-type: none"> <li>• This authority may be used to obtain “<b>any tangible things (including books, records, papers, documents, and other items).</b>” This authority is broad, similar in scope to a criminal grand jury subpoena.</li> <li>• This authority requires additional procedures for certain special categories of records (see below).</li> </ul>
<p>Special Categories of Tangible Things:</p>	<p>Congress designated particular categories of records for special procedures and approvals. The FBI will adjust procedures to account for the special designation.</p>
<p>• Special Categories:</p>	<p>Library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, and medical record containing information that would identify a person.</p>
<p>• Approval Level for special categories:</p>	<p>The Director of the FBI may delegate the authority to either –</p> <ul style="list-style-type: none"> <li>• the <b>Deputy Director</b> of the FBI; or</li> <li>• the <b>Executive Assistant Director (EAD) for National Security</b> (or any successor position).</li> </ul> <p><b>No further delegation is allowed.</b></p>
<p>• Congressional Oversight of special categories:</p>	<p>Attorney General must provide annual report (April) to the House Judiciary Committee (HJC), the House Permanent Select Committee on Intelligence (HPSCI), the Senate Judiciary Committee (SJC), and the Senate Select Committee on Intelligence (SSCI).</p> <ul style="list-style-type: none"> <li>• Number of FISA business record orders granted, modified, or denied for the special categories of tangible things.</li> </ul>

---

<sup>1</sup> This information also includes the changes made by sections 3 and 4 of the “USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006.”

UNCLASSIFIED

<p>FISA Business Record Standard- <b>Relevance:</b></p>	<p>The FBI's facts must show that there are "reasonable grounds to believe that the tangible things sought are <b>relevant to an authorized investigation.</b>"</p>
<p>• Presumptive Relevance Test:</p>	<p>The tangible things are presumptively relevant if the facts show they pertain to –                  "(i) a foreign power or an agent of a foreign power;                  (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or                  (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigations."</p>
<p>FISA Business Record Order:</p>	<ul style="list-style-type: none"> <li>• The order must describe the tangible things with <b>sufficient particularity</b> to permit them to be fairly identified.</li> <li>• <b>Date for return</b> - the order will contain a date on which the tangible things must be provided.</li> <li>• Recipient must have a <b>reasonable period of time</b> to produce.</li> <li>• The Order may only require production of tangible things that would be available with a grand jury subpoena or a District Court order (in other words, privileges under the law will apply to Business Record orders).</li> </ul>
<p>FISA Business Record Non-Disclosure Provision:</p>	<p>No person shall disclose the fact that the FBI has sought tangible things.</p>
<p>• Exceptions to non-disclosure:</p>	<p>A recipient may disclose a FISA Business Record Order to –                  (1) persons to whom disclosure is necessary to comply;                  (2) an attorney to obtain legal advice or assistance with respect to the production;                  (3) a person as permitted by the FBI Director (or designee).</p>
<p>• Extension of nondisclosure to others:</p>	<ul style="list-style-type: none"> <li>• If the recipient discloses to another person (see exceptions above), the recipient shall notify the person of the nondisclosure requirement.</li> <li>• The person to whom disclosure is made shall be subject to the nondisclosure requirement.</li> <li>• The FBI director (or designee) may ask the recipient to identify the other persons to whom disclosure of the Business Record order will be made (<b>except that the recipient does not have to identify the attorney</b>).</li> </ul>

UNCLASSIFIED

Judicial Challenge of FISA Business Record authority:	The recipient of a FISA Business Record order may challenge the legality of the order in the Foreign Intelligence Surveillance Court.
• Challenging the order:	<ul style="list-style-type: none"> <li>• Recipient may move to modify or set aside the order.</li> <li>• FISC may grant the motion only if the order does not meet the requirements of FISA or is otherwise unlawful.</li> </ul>
• Challenging the non-disclosure provision:	<ul style="list-style-type: none"> <li>• Not less than 1 year after the order, the recipient may move to modify or set aside the nondisclosure order.</li> <li>• FISC may grant such a motion only if there is no reason to believe that disclosure may endanger the national security of the U.S., interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.</li> <li>• The FISC will treat as conclusive a <b>certification</b> by the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the FBI that a disclosure may endanger the national security of the U.S., interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.</li> </ul>
• Security:	<ul style="list-style-type: none"> <li>• Filings shall be under seal</li> <li>• Chief Justice of the U.S., in consultation with the AG and the DNI, will establish security measures.</li> </ul>

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

Reporting Cycle:	Attorney General will report on an annual basis (April of each year).
------------------	---

UNCLASSIFIED

<p><b>Congressional Committees:</b></p>	<ul style="list-style-type: none"> <li>•House Permanent Select Committee on Intelligence</li> <li>•House Judiciary Committee</li> <li>•Senate Select Committee on Intelligence</li> <li>•Senate Judiciary Committee</li> </ul>
<p><b>Reporting Categories:</b></p>	<p>(1) Total number of applications for FISA Business Records.                  (2) Total number of orders granted, modified, or denied.                  (3) Total number of orders granted, modified, or denied for the special categories of tangible things.</p> <ul style="list-style-type: none"> <li>• Library circulation records, library patron lists, book sales records, or book customer lists.</li> <li>• Firearms sales records.</li> <li>• Tax return records.</li> <li>• Educational records.</li> <li>• Medical records containing information that would identify a person.</li> </ul>
<p><b>Additional unclassified report:</b></p>	<p>Annually (April of each year), the Attorney General shall make an unclassified report on the total number of FISA Business Records applications, and the total number of orders granted, modified, or denied.</p>

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

<p><b>Scope of Audit:</b></p>	<p>The IG will perform a comprehensive audit of the effectiveness and use, including any improper or illegal use, of the investigative authority.</p>
<p><b>Timing of Audit:</b></p>	<p>For 2002, 2003, and 2004, the audit should be completed within one year of enactment (March 9, 2007).</p> <p>For 2005 and 2006, the audit should be completed by December 31, 2007.</p>



UNCLASSIFIED

Report results to Congress:	The IG shall submit the audit reports to – <ul style="list-style-type: none"><li>• House Judiciary Committee.</li><li>• House Permanent Select Committee on Intelligence.</li><li>• Senate Judiciary Committee.</li><li>• Senate Select Committee on Intelligence.</li></ul>
Examine effectiveness of the tool:	Audit will look at the following for effectiveness – <ul style="list-style-type: none"><li>• Categories of records obtained.</li><li>• The importance to the FBI and the IC of the information obtained.</li><li>• The manner in which the information is collected, retained, analyzed, and disseminated by the FBI (this will include an examination of the access to “raw data” provided by the FBI to other agencies of the Federal, State, local, or tribal governments, or private sector agencies).</li><li>• The minimization procedures adopted by the AG.</li><li>• Whether, and how often, the FBI used information to produce analytical intelligence products for the FBI, the IC, or other Federal, State, local, or tribal government agencies.</li><li>• Whether, and how often, the FBI provided the information to law enforcement authorities for criminal proceedings.</li></ul>
Examine the process:	The audit process will look at the following: <ul style="list-style-type: none"><li>• How often the FBI requested DOJ to submit an application and the request was not submitted to the court (including the basis for the decision).</li><li>• Whether the court granted, modified, or denied the application.</li><li>• The justification for the failure of the AG to issue implementing procedures governing the requests in a timely fashion, including whether the delay harmed national security.</li><li>• Whether bureaucratic or procedural impediments prevent the FBI from fully using the authority.</li></ul>

**FISA ROVING SURVEILLANCE CHANGES**

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

UNCLASSIFIED

<p>Standard for roving surveillance:</p>	<ul style="list-style-type: none"> <li>• The FISC must find the possibility of the target thwarting surveillance based upon specific facts.</li> <li>• The order must describe the specific target in detail when authorizing a roving surveillance for a target whose identity is not known.</li> </ul>
--	--

<p>Return requirement:</p>	<ul style="list-style-type: none"> <li>• Presumed <b>10 day notice</b> – the FBI (applicant) must provide notice to the court within 10 days unless the court finds good cause to justify a longer period of up to 60 days.</li> </ul> <p>The FBI must inform the court:</p> <ul style="list-style-type: none"> <li>• The nature and location of new facility.</li> <li>• The facts and circumstances relied upon by applicant.</li> <li>• Any new minimization procedures.</li> <li>• The total number of electronic surveillances that have been or are being conducted under the roving authority.</li> </ul>
----------------------------	--

<p>Reporting cycle:</p>	<p>The Attorney General will report on a semi-annual basis.</p>
<p>Congressional Committees:</p>	<ul style="list-style-type: none"> <li>• House Permanent Select Committee on Intelligence</li> <li>• Senate Select Committee on Intelligence</li> <li>• Senate Judiciary Committee</li> </ul>
<p>Reporting categories:</p>	<ul style="list-style-type: none"> <li>• Total number of applications made for orders and extensions.</li> <li>• Each criminal case in which information has been authorized for use at trial, during the period covered by such report.</li> <li>• Total number of emergency employments and total number of subsequent orders approving or denying surveillance.</li> </ul>

**FISA OVERSIGHT CHANGES**

<p>Reporting cycle:</p>	<p>Attorney General will report on a semiannual basis.</p>
<p>Congressional Committees:</p>	<ul style="list-style-type: none"> <li>• House Permanent Select Committee on Intelligence</li> <li>• House Judiciary Committee</li> <li>• Senate Select Committee on Intelligence</li> <li>• Senate Judiciary Committee</li> </ul>

UNCLASSIFIED

<p>Reporting categories:</p>	<p>Report the following regarding emergency physical searches –</p> <ul style="list-style-type: none"> <li>• Total number of applications.</li> <li>• Total number of orders granted, modified, or denied.</li> <li>• Number of physical searches involving the residences, offices, or personal property of U.S. persons, and the number of occasions the AG provided notice.</li> <li>• Total number of emergency authorizations, and total number of subsequent orders approving or denying the physical searches.</li> </ul>
------------------------------	--

<p>Reporting cycle:</p>	<p>Attorney General will report on a semiannual basis.</p>
<p>Congressional Committees:</p>	<ul style="list-style-type: none"> <li>• House Permanent Select Committee on Intelligence</li> <li>• House Judiciary Committee</li> <li>• Senate Select Committee on Intelligence</li> <li>• Senate Judiciary Committee</li> </ul>
<p>Reporting categories:</p>	<p>Report the following regarding pen registers/trap and trace –</p> <ul style="list-style-type: none"> <li>• Total number of applications.</li> <li>• Total number of orders granted, modified, or denied.</li> <li>• Total number of emergency authorizations, and total number subsequent orders approving or denying the pen registers/trap and trace.</li> </ul>

**FISA PEN REGISTER/TRAP AND TRACE CHANGES**

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

UNCLASSIFIED

<p>Customer/subscriber using the service covered:</p>	<p>Information available through PR/TT:</p> <ul style="list-style-type: none"> <li>• Name of the customer or subscriber.</li> <li>• Address of the customer or subscriber.</li> <li>• Telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission information.</li> <li>• Length of service.</li> <li>• Types of service.</li> <li>• Any local or long distance telephone records of the customer/subscriber.</li> <li>• Records reflecting period of usage.</li> <li>• Mechanisms/sources of payment, including the number of any credit card or bank account used.</li> </ul>
<p>Customer/subscriber of incoming or outgoing communications to/from the service covered:</p>	<p>Information available through PR/TT:</p> <ul style="list-style-type: none"> <li>• Name of customer/subscriber.</li> <li>• Address of customer/subscriber.</li> <li>• Telephone or instrument number, or other subscriber number or identifier, ... including any temporarily assigned network address or associated routing or transmission information.</li> <li>• Length of service.</li> <li>• Types of service.</li> </ul>
<p>Reporting cycle:</p>	<p>Attorney General shall report on a semiannual basis.</p>
<p>Congressional Committees:</p>	<ul style="list-style-type: none"> <li>• House Permanent Select Committee on Intelligence</li> <li>• House Judiciary Committee</li> <li>• Senate Select Committee on Intelligence</li> <li>• Senate Judiciary Committee</li> </ul>
<p>Reporting categories:</p>	<p>Use of pen registers and trap and trace.</p>

**EMERGENCY DISCLOSURES**

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

UNCLASSIFIED

Voluntary disclosure by provider:	If the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay.
Reporting cycle:	Attorney General shall report on an annual basis.
Congressional Committees:	<ul style="list-style-type: none"> <li>• House Judiciary Committee</li> <li>• Senate Judiciary Committee</li> </ul>
Reporting categories:	<ul style="list-style-type: none"> <li>• Number of accounts from which voluntary disclosures were received.</li> <li>• Summary of the basis for disclosure where the investigation was closed without criminal charges.</li> </ul>

NATIONAL SECURITY LETTERS

**Sec. 115. Judicial Review of National Security Letters.**

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

Judicial review of NSL non-disclosure provision (Recipient may challenge the non-disclosure provision):	• Jurisdiction: In the U.S. District in which the recipient resides or does business.
---	---

UNCLASSIFIED

	<ul style="list-style-type: none"><li>• Filed <b>within one year</b> of NSL request –</li><li>• Court may <b>modify/set aside</b> the non-disclosure if... “no reason to believe that disclosure may endanger the national security of the U.S., interfere with criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.”</li><li>• <b>Certification/Authority level:</b> Court will treat as conclusive the certification by the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the FBI that disclosure may endanger the national security of the United States or interfere with diplomatic relations (unless made in bad faith).</li></ul> <hr/> <ul style="list-style-type: none"><li>• Filed <b>one year or more</b> after the NSL –</li><li>• Within 90 days of recipient’s petition, designated government officials must either <b>terminate</b> the nondisclosure requirement or <b>recertify</b> that the disclosure “may result in a danger to the national security of the U.S., interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person.”</li><li>• <b>Termination/Recertification Authority level:</b> The Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the FBI, or his designee in a position not lower than Deputy Assistant Director at FBI headquarters or a SAC in an FBI field office designated by the Director.</li><li>• Certification that disclosure may endanger the national security of the United States or interfere with diplomatic relations conclusive (unless made in bad faith).</li></ul>
--	---

Failure to Comply:	<ul style="list-style-type: none"><li>• The Attorney General may invoke the aid of a Federal District Court.</li><li>• Jurisdiction: U.S. District in which the investigation is carried on, or the person or entity resides or does business or may be found.</li><li>• Court may compel by ordering person/entity to comply.</li><li>• Failure to obey is punishable by contempt.</li></ul>
--------------------	---

UNCLASSIFIED

<p>Court Proceedings &amp; Security:</p>	<ul style="list-style-type: none"> <li>• Court must close hearings to the extent necessary to prevent an unauthorized disclosure of NSL.</li> <li>• Petitions, filings, records, orders, and subpoenas must be kept <b>under seal</b> to the extent and as long as necessary to prevent unauthorized disclosure.</li> <li>• At government’s request, ex parte and in camera review of government’s submissions which may contain classified material.</li> </ul>
--	--

**Sec. 116. Confidentiality of National Security Letters.<sup>2</sup>**

<p>Nondisclosure activated by FBI Certification:</p>	<ul style="list-style-type: none"> <li>• <b>FBI certification:</b> There may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, if a recipient discloses that the FBI has sought or obtained access to information or records under NSL statutes.</li> <li>• <b>Authority level: Director of the FBI</b>, or his designee in a position not lower than <b>DAD at FBI headquarters</b>, or a <b>Special Agent in Charge in a Bureau field office designated by the Director</b>.</li> </ul>
<p>Exceptions - Recipient may disclose NSL request:</p>	<ul style="list-style-type: none"> <li>• Recipient may disclose to persons necessary to comply with NSL request.</li> <li>• <b>Attorney:</b> Recipient may disclose to an attorney to obtain legal advice or legal assistance regarding any NSL request.</li> </ul>
<p>Notice:</p>	<ul style="list-style-type: none"> <li>• The NSL shall notify the recipient of the nondisclosure requirement.</li> <li>• Recipient disclosing NSL to an individual necessary to comply or an attorney shall inform them of the applicable nondisclosure requirement.</li> </ul>
<p>FBI request for identity of persons to whom recipient plans to disclose NSL:</p>	<ul style="list-style-type: none"> <li>• Only activated at the request of the FBI Director or Director’s designee.</li> </ul>

<sup>2</sup> This information also includes the changes made by sections 4 and 5 of the “USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006.”

UNCLASSIFIED

	<ul style="list-style-type: none"> <li>• Recipient of NSL shall identify the persons to whom disclosure will be made or was made.</li> </ul>
	<ul style="list-style-type: none"> <li>• <b>EXCEPT:</b> Nothing requires the person to identify an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance.</li> </ul>

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

<p>Obstruction of an Investigation (18 U.S.C. § 1510):</p>	<ul style="list-style-type: none"> <li>• Individual must have been notified of the nondisclosure provision.</li> </ul>
	<ul style="list-style-type: none"> <li>• Individual must knowingly and with the intent to obstruct an investigation or judicial proceeding violate the nondisclosure provision.</li> </ul>
	<ul style="list-style-type: none"> <li>• Punishable by up to five years imprisonment, a fine, or both.</li> </ul>

**Sec. 118. Reports on National Security Letters.**

<p>Current NSL Reports:</p>	<ul style="list-style-type: none"> <li>• AG reports on a semi-annual basis.</li> </ul>
	<ul style="list-style-type: none"> <li>• Reports will now also be made to the House Judiciary Committee, the House Permanent Select Committee on Intelligence, the Senate Judiciary Committee, and the Senate Select Committee on Intelligence.</li> </ul>

<p>Enhanced Oversight of 15 U.S.C. § 1681v NSLs (for credit agency consumer records):</p>	<ul style="list-style-type: none"> <li>• AG reports on a semi-annual basis.</li> </ul>
	<ul style="list-style-type: none"> <li>• Reports will now also be made to the House Judiciary Committee, the House Committee on Financial Services, the House Permanent Select Committee on Intelligence, the Senate Judiciary Committee, the Senate Housing and Urban Affairs Committee, and the Senate Select Committee on Intelligence.</li> </ul>

<p>Aggregate Report of NSL requests:</p>	<ul style="list-style-type: none"> <li>• AG reports annually (April).</li> </ul>
	<ul style="list-style-type: none"> <li>• Total number of NSL (excluding NSLs for subscriber information) requests for information concerning <u>different</u> U.S. persons.</li> </ul>



UNCLASSIFIED

	<ul style="list-style-type: none"> <li>• Unclassified report.</li> </ul>
--	--

**Sec. 119. Enhanced Oversight of National Security Letters.**

<p>Requirements of DOJ IG Audit:</p>	<p>Comprehensive audit of --</p> <ul style="list-style-type: none"> <li>• Use of NSLs for 2003 through 2006.</li> <li>• Description of noteworthy facts/circumstances, including any improper or illegal use of NSLs.</li> </ul>
<p>Timing of Audit:</p>	<ul style="list-style-type: none"> <li>• For 2003 and 2004, must be completed not later than one year after enactment (March 9, 2007).</li> <li>• For 2005 and 2006, must be completed not later than December 31, 2007.</li> </ul>
<p>Examine Effectiveness of NSLs:</p>	<p>The audit will examine:</p> <ul style="list-style-type: none"> <li>• Importance of the information acquired by DOJ to the intelligence activities of DOJ and other members of the IC.</li> <li>• How information is collected, retained, analyzed, and disseminated (including access to raw data) to members of the IC community, and other Federal, State, local or tribal governments, or private sector entities.</li> <li>• How often NSL information was used to produce an analytical intelligence product for distribution to the IC community, and to other Federal, State, local or tribal governments.</li> <li>• Whether, and how often, NSL information was provided to law enforcement authorities for use in criminal investigations.</li> <li>• Following enactment of the USA PATRIOT IRA, the number of NSLs issued without the certification necessary to create a nondisclosure obligation.</li> <li>• Types of electronic communications and transactional information obtained under § 2709, and the procedures DOJ used if content information is obtained.</li> </ul>
<p>Feasibility of Minimization Procedures:</p>	<ul style="list-style-type: none"> <li>• Not later than February 1, 2007, or upon completion of the 2003/2004 audit, the Attorney General and the Director of National Intelligence shall jointly submit a report on the feasibility of applying minimization procedures to protect the constitutional rights of U.S. persons.</li> <li>• Report goes to the House Judiciary Committee, the House Permanent Select Committee on Intelligence, the Senate Judiciary Committee, and the Senate Select Committee on Intelligence.</li> </ul>

UNCLASSIFIED

**DELAYED NOTICE SEARCH WARRANTS**

**Sec. 114. Delayed Notice Search Warrants.**

Notification Delay	No more than <b>30 days</b> (or a later date certain if facts justify).
Extensions of Delays	<b>90 days</b> (unless the facts justify longer)-- <ul style="list-style-type: none"><li>•granted upon an updated showing of the need for further delay.</li><li>•undue delay of trial is not a basis for a delayed notice.</li></ul>
Reporting	Annual reporting to Congress by Court (starting with the fiscal year ending September 30, 2007).

**DATA-MINING ACTIVITIES**

**Sec. 126. Report on Data-Mining Activities.**

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

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

(1) Data-Mining.—The term “data-mining” means a query or search or other analysis of one or more electronic databases, where—

(A) at least one of the databases was obtained from or remains under the control of a non-Federal entity, or the information was acquired initially by another department or agency of the Federal Government for purposes other than intelligence or law enforcement;

(B) the search does not use personal identifiers of a specific individual or does not utilize inputs that appear on their face to identify or be associated with a specified individual to acquire information; and

(C) a department or agency of the Federal Government is conducting the query or search or other analysis to find a pattern indicating terrorist or other criminal activity.

UNCLASSIFIED

17

NSL VIO-34825

FEDERAL BUREAU OF INVESTIGATION  
FOIPA  
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 87

Page 1 ~ Referral/Direct

Page 2 ~ Referral/Direct

Page 3 ~ Referral/Direct

Page 4 ~ Referral/Direct

Page 5 ~ Referral/Direct

Page 6 ~ b5

Page 7 ~ b5

Page 8 ~ b5

Page 9 ~ b5

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

Page 38 ~ Duplicate

Page 39 ~ Duplicate

Page 40 ~ Duplicate

Page 41 ~ Duplicate

Page 42 ~ Duplicate

Page 43 ~ Duplicate

Page 44 ~ Duplicate

Page 45 ~ Duplicate

Page 46 ~ Duplicate

Page 47 ~ Duplicate

Page 48 ~ Duplicate

Page 49 ~ Duplicate

Page 50 ~ Duplicate

Page 51 ~ Duplicate

Page 52 ~ Duplicate

Page 53 ~ Duplicate

Page 54 ~ Duplicate

Page 55 ~ Duplicate

Page 56 ~ Duplicate

Page 57 ~ Duplicate

Page 58 ~ Duplicate

Page 59 ~ Duplicate

Page 60 ~ Duplicate

Page 61 ~ Duplicate

Page 62 ~ Duplicate

Page 63 ~ Duplicate  
Page 64 ~ Duplicate  
Page 65 ~ Duplicate  
Page 66 ~ Duplicate  
Page 67 ~ Duplicate  
Page 68 ~ Outside the Scope  
Page 69 ~ Outside the Scope  
Page 70 ~ Outside the Scope  
Page 71 ~ Outside the Scope  
Page 78 ~ Duplicate  
Page 79 ~ Duplicate  
Page 106 ~ b5  
Page 107 ~ b5  
Page 108 ~ b5  
Page 109 ~ b5  
Page 110 ~ b5  
Page 111 ~ b5  
Page 112 ~ b5  
Page 113 ~ b5  
Page 114 ~ b5  
Page 115 ~ b5  
Page 116 ~ b5  
Page 117 ~ b5  
Page 118 ~ b5  
Page 119 ~ b5  
Page 120 ~ b5  
Page 121 ~ b5  
Page 122 ~ b5  
Page 123 ~ b5  
Page 124 ~ b5  
Page 125 ~ b5  
Page 126 ~ b5  
Page 127 ~ b5  
Page 128 ~ b5  
Page 129 ~ b5  
Page 130 ~ b5  
Page 131 ~ b5  
Page 132 ~ b5  
Page 133 ~ b5  
Page 134 ~ b5  
Page 135 ~ b5  
Page 136 ~ b5  
Page 137 ~ b5