National Security Letters

National Security Law Branch
Federal Bureau of Investigation

1

Slides take into acct the changes (eff. 9 Mar 06) resulting fm USA PATRIOT Act's reauthorization.

National Security Letters

- Prior to 2001 Patriot Act, standard for getting NSL was that the target be tied to foreign power.
- Under Section 505 of the Patriot Act, lesser standard – only need the information to be "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States."
- Can get NSL in [redacted] investigation
- Subject of NSL does not need to be target of investigation, as long as expected information is relevant to authorized investigation

3

b1
b2
b7E

9 Mar 06 Δ's

National Security Letters

- Prior to 2001 USA PATRIOT Act, approval authority could be no lower than Deputy Assistant Director; PATRIOT Act allowed delegation down to the SACs.
- As of March 9, 2006, approval authority has been delegated to
  - Deputy Director
  - Executive Assistant Director and Assistant EAD for National Security Branch
  - Assistant Directors and all DADs for CI/CT/Cyber
  - General Counsel
  - Deputy General Counsel for National Security Law Branch
  - Assistant Director in Charge, and all SACs in NY, D.C., and LA
  - All SACs in other field divisions
- Personnel in acting positions cannot sign NSLs.
- If do not have SAC in field office, can send EC to NSLB requesting that we draft the NSL and send it out

4

National Security Letters

- For all NSLs, issuing office must prepare two documents: (1) the NSL itself; and (2) an EC approving the NSL and documenting the factual predicate for the NSL
- All NSLs must be addressed to the specific company point of contact (many of which are listed on NSLB's website)
- All NSLs should identify the statutory authority for the request, the type of records requested, and provide identifying information to assist the company in processing the request. The NSL should "direct" the recipient to produce the information – that is a change from previous forms, which only "requested" the information.
- All NSLs require a certification that the records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities and that an investigation of a USP is not conducted solely on the basis of First Amendment rights.

5

9 Mar 06 Δ's

National Security Letters – new provisions

- CHANGES under USA PATRIOT Improvement and Reauthorization Act of 2005 (enacted into law March 9, 2006):
- A certification of the necessity for a non-disclosure provision is required in order for the NSL to include such a provision
  - Disclosure 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
- Such certification authority has been delegated to the same persons who have signature authority
- All NSLs should give notice of right of NSL recipient to challenge NSL in district court if production is unreasonable, oppressive or otherwise unlawful
- NSLs should give notice of right to challenge non-disclosure provision, if such provision is included in NSL

6

9 Mar 06 A's

National Security Letters – new provisions

- If non-disclosure provision challenged within one year, district court can modify provision if no reason to believe danger will ensue, unless Director certifies to such danger – such certification taken as conclusive unless made in bad faith
- If non-disclosure provision challenged one year or later, those parties with certification authority also have been delegated authority to recertify as to the harm that may ensue from disclosure.
- Even under non-disclosure provision, recipient can disclose to those in company who have need to know, as long as those persons are given notice of non-disclosure provision, and can disclose to lawyers for legal advice. FBI can request names of persons, except lawyers, who were given that information.
- All NLS should give notice of right of USG to enforce NSL (5 year penalty if violate non-disclosure provision intentionally for purpose of obstructing justice; contempt of court for violating order to produce)

7

National Security Letters

- Certain NSLs have an attachment suggesting the type of information that the company may considered to fall within the parameters of the statute. For example:
  - Toll billing records
  - Financial records
  - ISP – exhaustive list of types of transactional records available for production

9

b2
b7E

QUESTIONS?

- NSLB - (202) 324-[redacted]
- [redacted]

b6
b7C
b2

20

NSLs, infra.

[redacted] OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Thursday, March 30, 2006 10:58 AM
To: [redacted] (OGC) (FBI)
Subject: FYI: FBI Legislative Proposals

UNCLASSIFIED
NON-RECORD

[redacted]

b6 Per your request at this morning's NSLPTU Meeting, I'm attaching the FBI's legislative proposals and
b7C DOJ's comments regarding them.

Also, in the e-mail below, you'll see answers to two of the follow-on questions posed by Margaret Pittman in ODNI's OGC.

FYI.

[redacted]

FBI Rsp to ODNI datacall.pdf (...

DOJ comments re fbi proposals....

-----Original Message-----
From: [redacted] OGC) (FBI)
Sent: Wednesday, March 29, 2006 5:02 PM
To: [redacted] (OCA) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: ODNI Questions re FBI Legislative Proposals

UNCLASSIFIED
NON-RECORD

b6
b7C [redacted]

As you requested, I'm responding to Margaret Pittman of ODNI's OGC regarding two of her questions involving the FBI's legislative proposals.

As you and I discussed this afternoon, I've information on two different computer systems--my FBI Intranet account and my Internet Cafe account. With a view toward consolidating it in one answer on one account, I'm sending the answers to you FYI. Then, I intend to FAX a hard copy to Margaret at ODNI to respond to her questions.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-31-2007 BY 65179dmh/ksl/lmf

Margaret's questions and NSLB's answers follow:

estion No. 1

[redacted] b5

Answer No. 1

[redacted] b5

Question No. 2

[redacted]his is going to sound really obvious- [redacted] b5

swer No. 2

b6 b7C Thanks to [redacted] who provided the comments below.

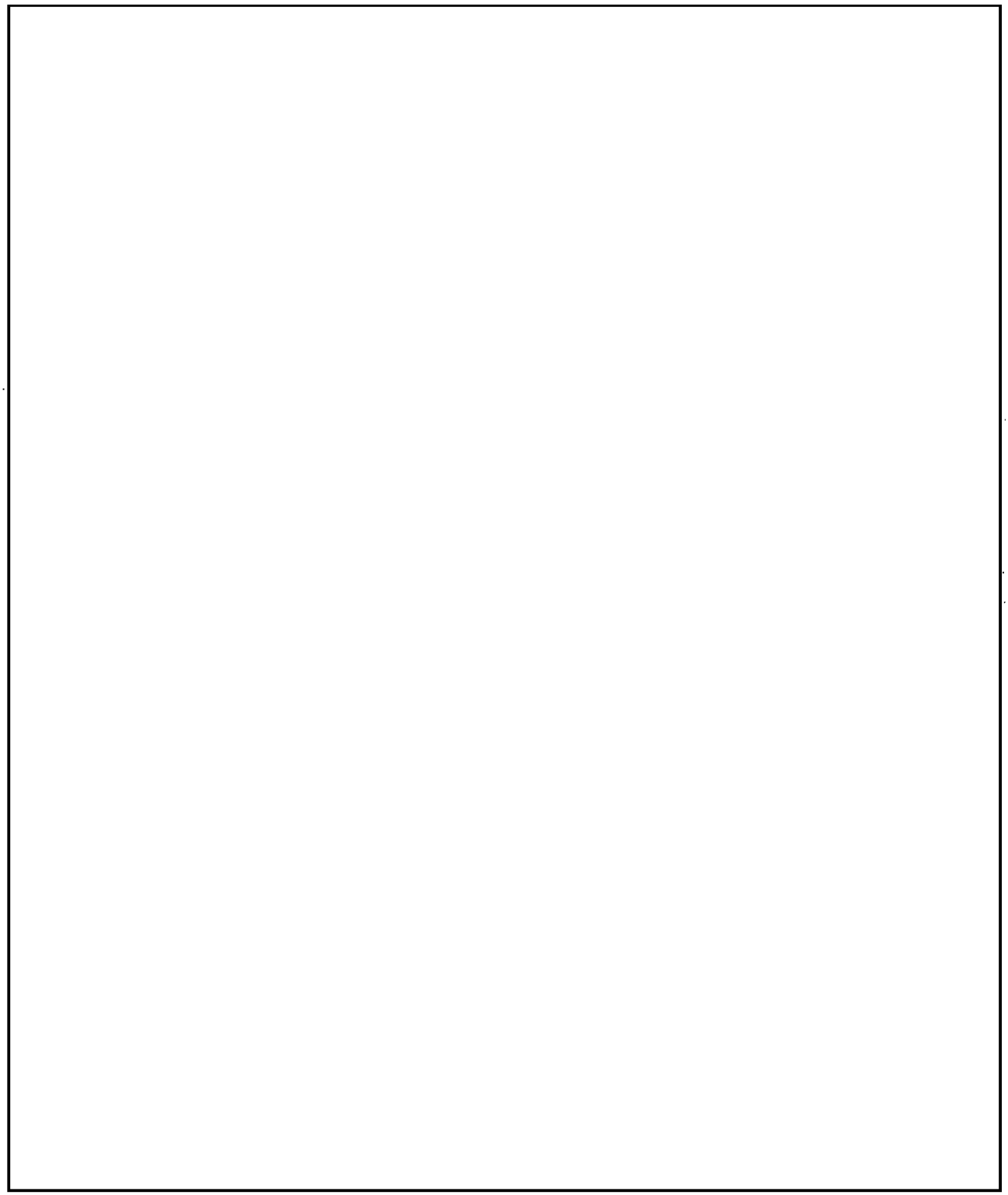
[redacted] b5

b5

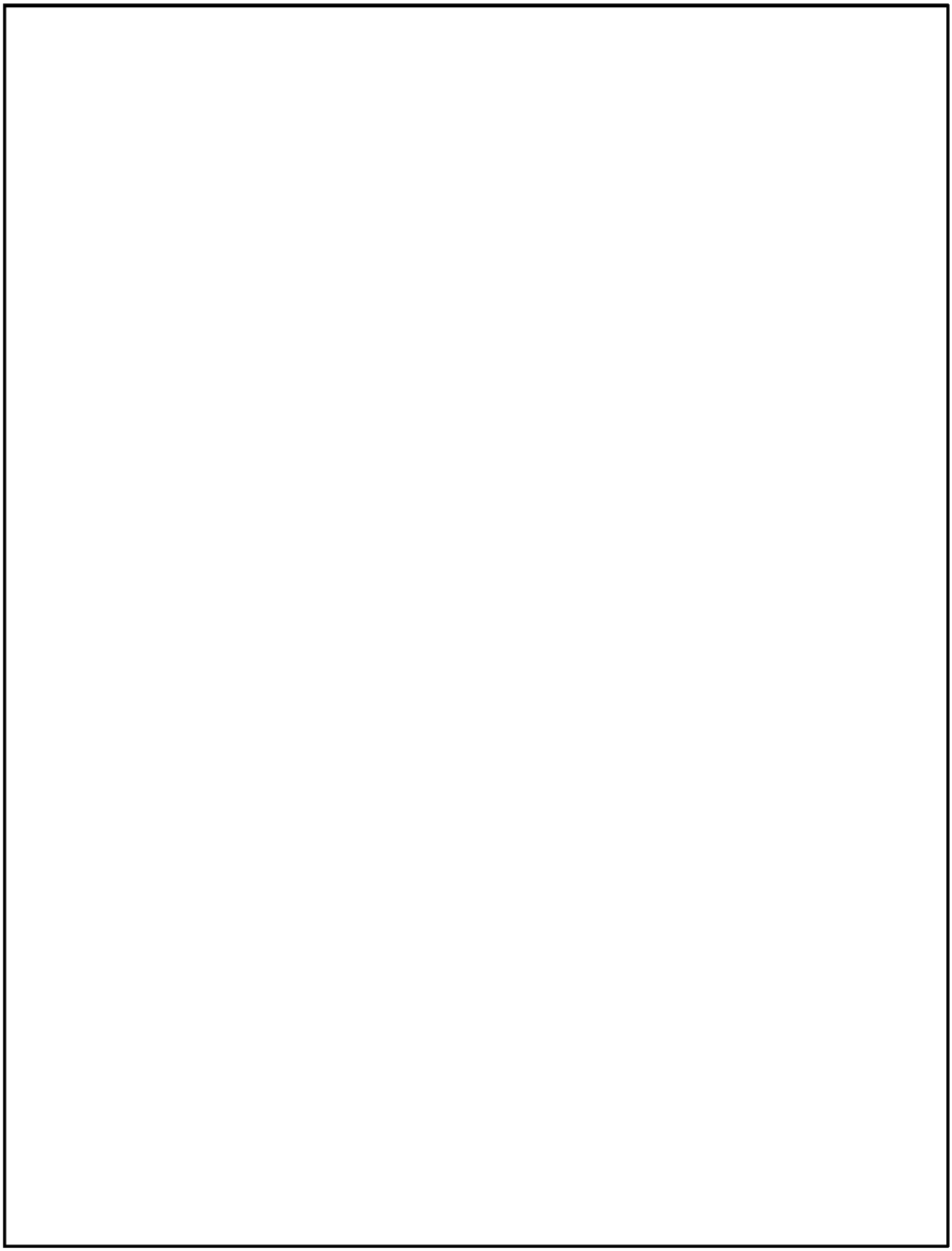
I trust the above will assist. But, if additional information is needed, we'll be glad to give it another shot.

b6
b7C

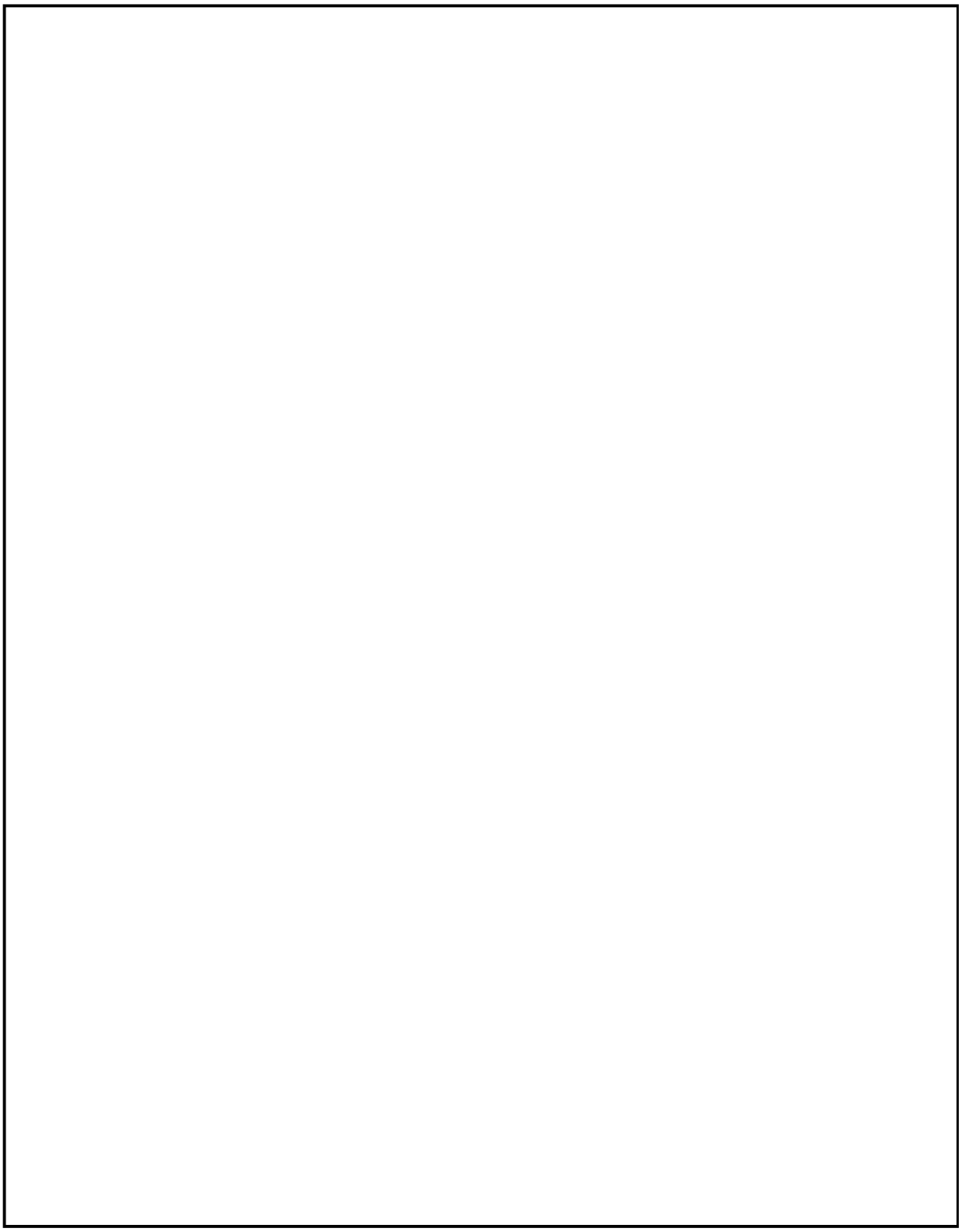
UNCLASSIFIED



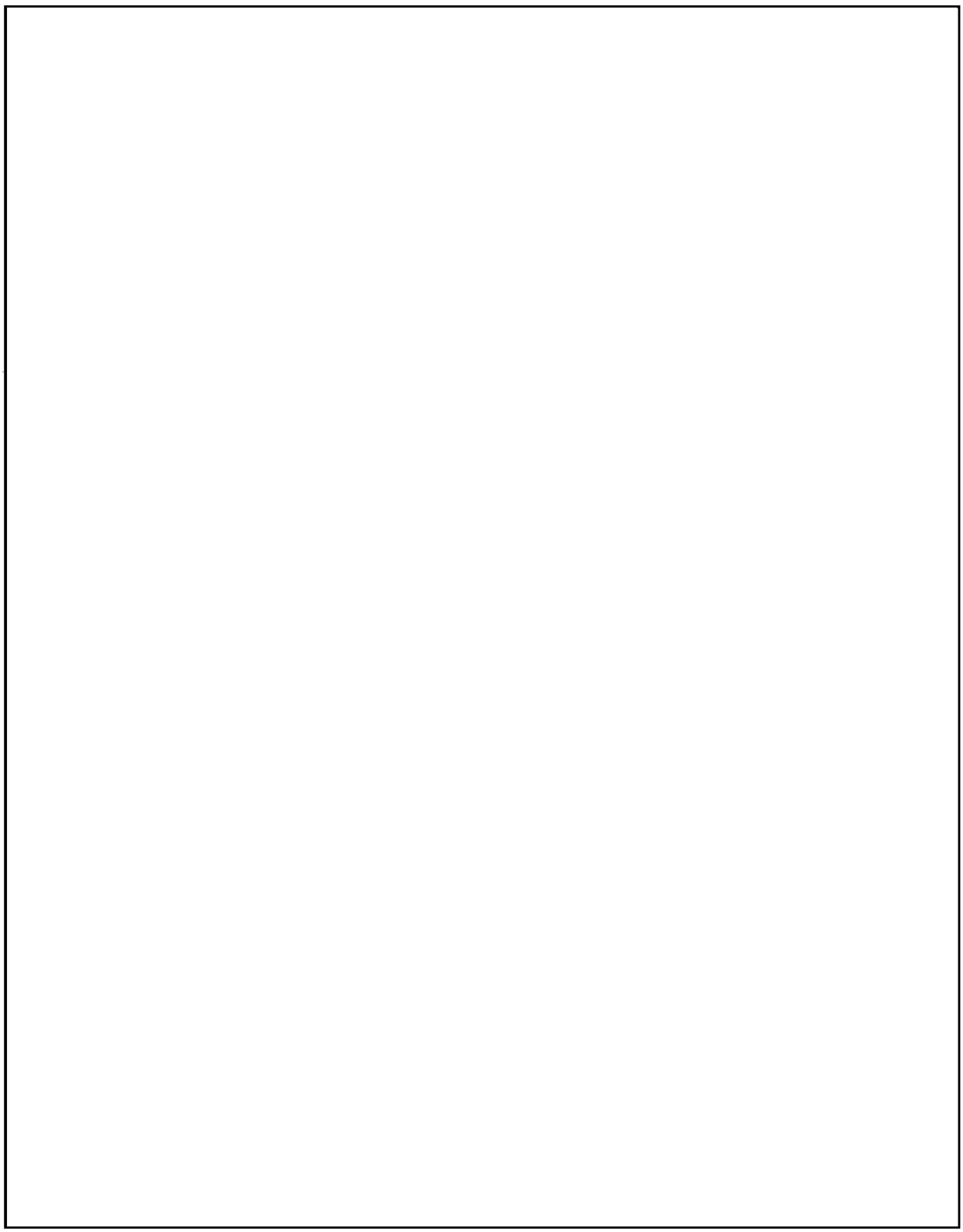
b5



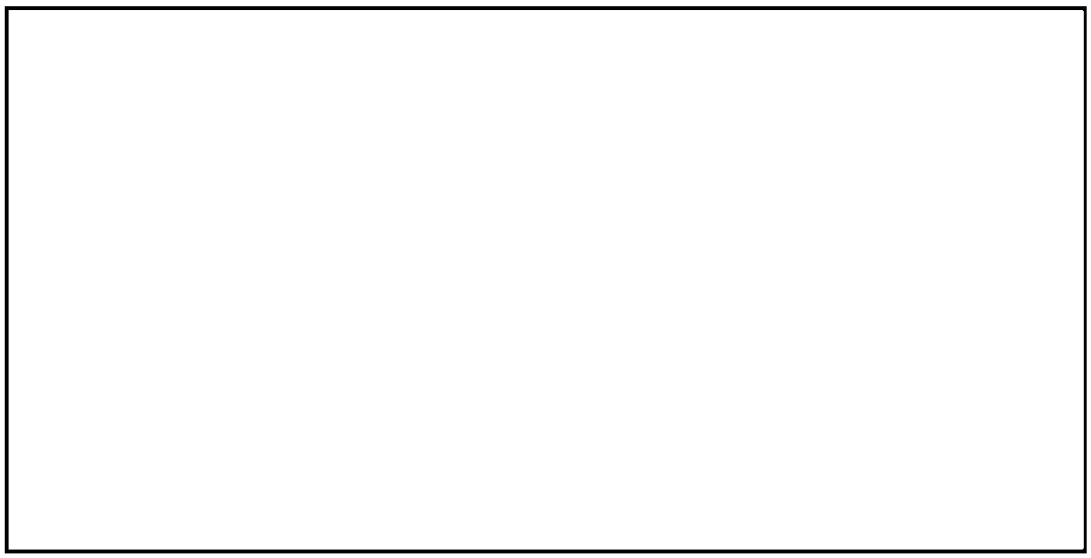
b5



b5

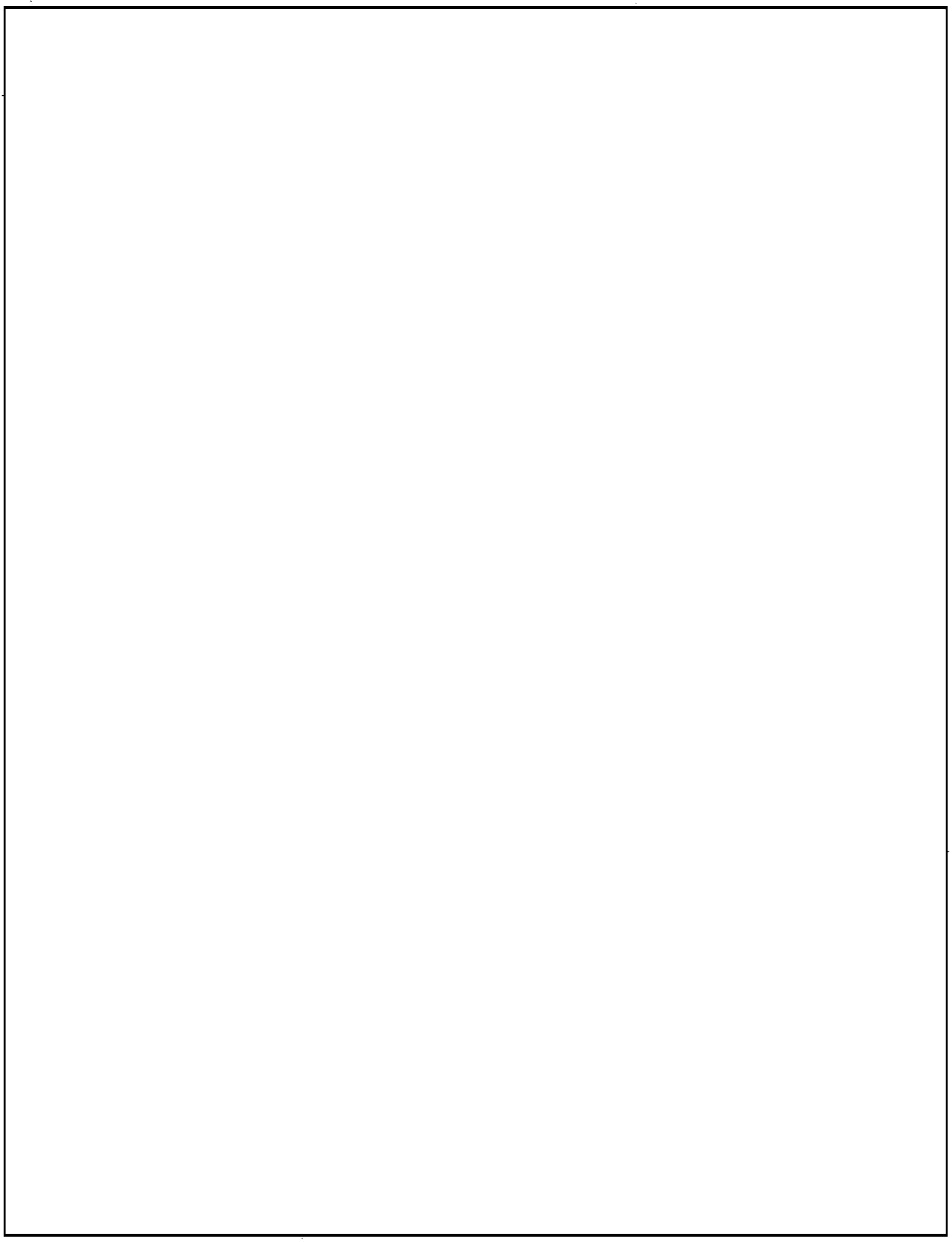


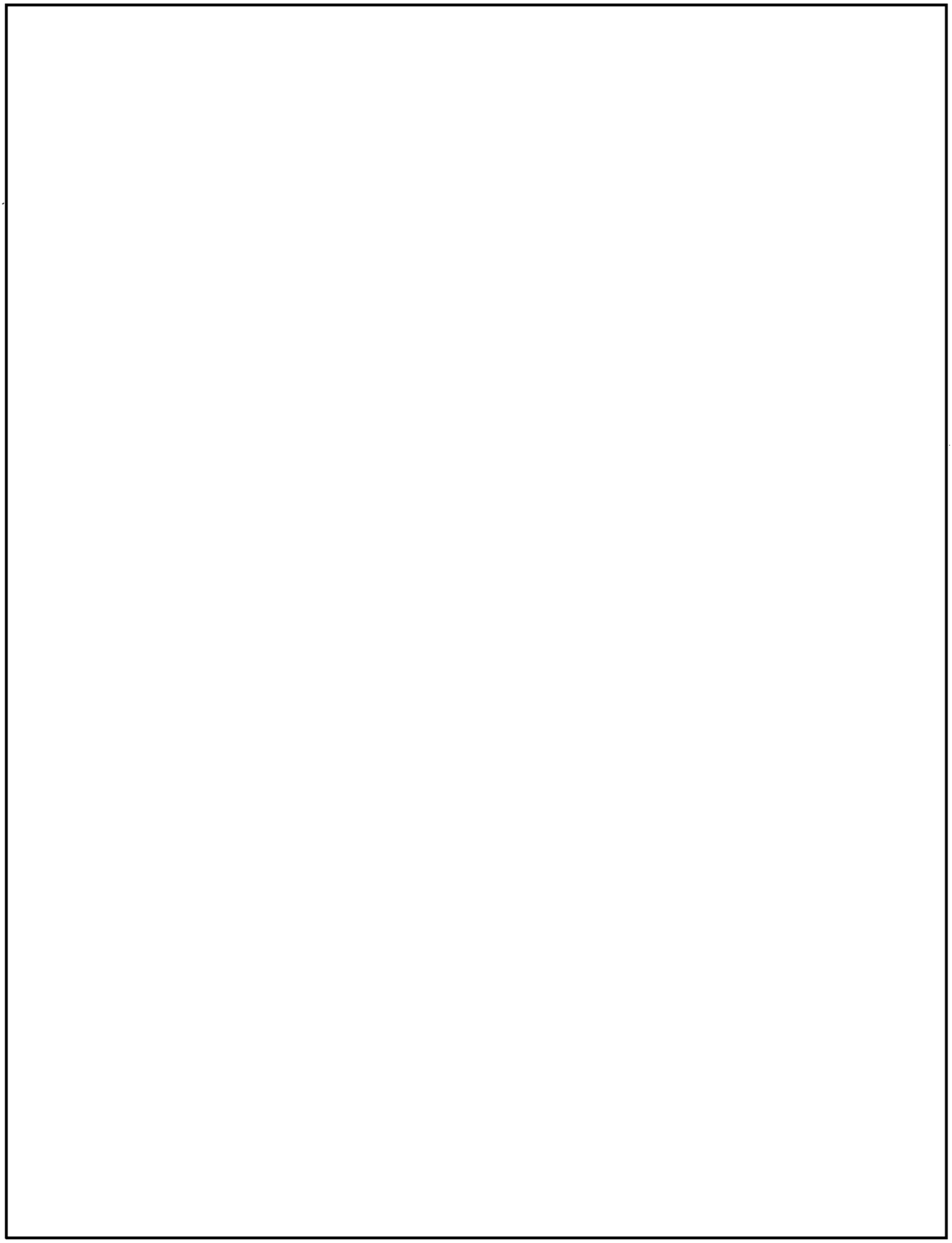
b5

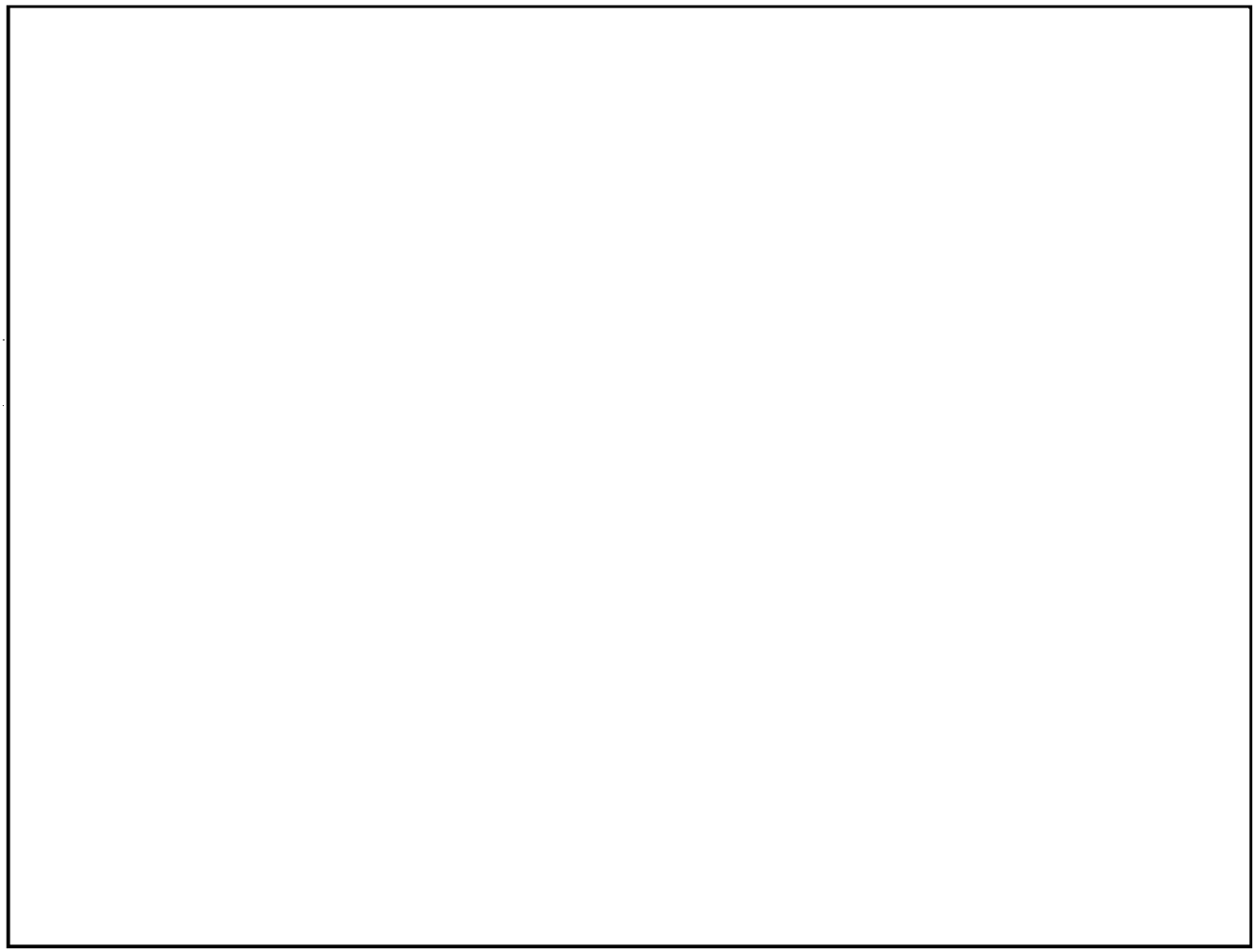


b5

Comments from Justice Department Components
on FBI Response to ODNI Request for Intelligence Authorization Proposals







(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/01/2007

To: All Divisions **Attn:** ADIC/SAC
CDC
Attn: Manual's Desk

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

b6
b7C
b2

Approved by: Pistole John S
Caproni Valerie E

Drafted By: [redacted]

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

Title: LEGAL ADVICE AND OPINIONS;
TELEPHONE QUERIES;
EMERGENCY DISCLOSURE PROVISION

Synopsis: 1) Provides comprehensive guidance on the investigative techniques available to obtain subscriber and toll billing records.

2) Provides guidance that information should not be obtained from wire or electronic communications service providers upon the issuance of an "exigent letter," i.e., a written promise to provide future legal process.

3) Directs all divisions to cease the practice of using "exigent letters."

4) Provides updated guidance concerning the emergency disclosure provision in 18 U.S.C. § 2702.

Attachment:

Sample Emergency Disclosure Letter

Details:

After reviewing information provided to it in the course of the Congressionally-mandated Office of Inspector General's audit of the FBI's use of National Security Letters (NSLs), the Office of the General Counsel (OGC) provides this clarification of the legal avenues available to investigators who seek to obtain subscriber information and toll billing information from telephone companies.[1]

[1] While the circumstance that was the genesis of this EC involved the gathering of telephone information, the discussion herein as to the use of exigent letters, national security letters, and emergency disclosure letters

When an FBI employee wishes to obtain subscriber or other information about a telephone number, it is incumbent upon the employee to develop or obtain a sufficient factual predicate to allow for the lawful acquisition of this information. Investigators should cease the practice of obtaining such information from wire communications service providers in advance of and upon the promise of the issuance of legal process. In case of a true emergency, they should use another investigative technique to obtain that information. See discussion below.

National Security Letter and Grand Jury Subpoena:

If a telephone number is known to be related to an existing national security investigation and if the information sought will be relevant to that investigation, a national security letter (NSL) may be issued to a wire communications service provider pursuant to 18 U.S.C. § 2709 in order to obtain subscriber or toll billing records about that telephone number.[2] Further, if there is a criminal nexus to the national security investigation, as well as in a purely criminal investigation, a grand jury subpoena can be used to obtain the same information. In either instance - a national security letter or a grand jury subpoena - a copy of the signed legal process should be maintained in the investigative file. To date, there has been no such requirement with respect to national security letters. Additional guidance will be forthcoming which will require retention of signed copies of NSLs and require documented proof of service of such letters.

Emergency Disclosure Letter:[3]

If there is not sufficient time to obtain a grand jury subpoena or to issue an NSL in advance of the need for the information, then the information may be sought through emergency voluntary disclosure pursuant to 18 U.S.C. § 2702 (c)(4). The statute provides for the disclosure of customer records "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." 18 U.S.C. § 2702

---

applies equally to electronic communications transactional records obtained from electronic communication service providers.

[2] Obviously, 18 U.S.C. § 2709 also allows the FBI to obtain electronic transactional communications records from electronic communications service providers.

[3] This discussion applies to both national security investigations and criminal investigations.

(c)(4). Further, content information[4] may also be disclosed voluntarily by the service provider, under the same standard. See 18 U.S.C. § 2702(b)(8).[5] In such a situation, which is likely to be rare, the FBI should relay the facts to the provider and ask that it make a determination that there is an emergency situation justifying disclosure of the requested information. There is no further legal process necessary. See discussion below.

An emergency disclosure letter may be used in situations when [redacted] b5

Although case law has yet to be fully developed to help define when an emergency situation exists, the legislative history provides some insight. For instance,

> "[i]f someone plans to bomb an elementary school next week, then the communications provider should be able to disclose that information and not have to guess whether an action which is to occur a week later constitutes 'an immediate' danger or not. In such case, law enforcement may need all

[4] The distinction between customer records and content information may not always be clear, particularly in the context of electronic communications. [redacted] b5 NSLB intends to provide further clarification of the use of those terms on its website.

[5] Section (c)(4) was amended by the USA Patriot Act Improvement and Reauthorization Act of 2005 (Reauthorization Act) to make its language identical to that of Section (b)(8). Prior to the Reauthorization Act, Section (c)(4) required a reasonable belief by the service provider as to the existence of an emergency requiring disclosure of the information, and also required that there be an "immediate" danger of death or serious bodily injury. The Reauthorization Act eliminated the "immediate" requirement, and also provided that the service provider need only have a "good faith" basis for the belief that disclosure is required.

> the time it can get to locate the perpetrator and prevent the crime. Another example is where an individual sends an e-mail to another person describing an upcoming terrorist attack he or she is planning but does not put a date on the attack. A terrorist attack would clearly constitute an emergency that threatens life or limb, but the timing of the attack may not be evident. The attack could be planned for tomorrow or for a year from now. It is clear that there is a danger, but the immediacy of that danger is unclear."[6]

Both of these examples illustrate emergency situations because they demand immediate *action* as opposed to creating an immediate *danger*. As demonstrated by the example of the upcoming attack, even if the timing of the attack is unknown, immediate action is required to spare life and limb. Thus, the threshold requirement for this provision is that the situation demands immediate action to prevent death or serious bodily injury.

Sufficient facts must be developed that would lead not only the FBI but a service provider to believe, in good faith, that disclosure of the information sought is required without delay by an emergency situation involving the danger of death or serious physical injury to any person. [redacted] b5 [redacted] Disclosure under this provision is voluntary. A service provider cannot be forced to provide information under this provision. Because the disclosure is voluntary, it is unnecessary and contrary to the statute for the voluntary disclosure to be followed by any legal process. The determination by the service provider that an emergency situation exists is the legal justification for the disclosure.

Use of this provision must be approved at a level not lower than ASAC in a field office and not lower than Section Chief at Headquarters. While the approval may be oral, the better practice is that the approval be written, in the form of a signature on the letter to the service provider. A sample letter is attached. If the approval is oral, however, a summary setting forth the facts creating the emergency condition must be documented in writing and signed by

---

[6] See House Report No. 107-497, pp.13-14, dated June 11, 2002, accompanying H.R. 3482, the "Cyber Security Enhancement Act of 2002," which passed as a part of the comprehensive Homeland Security Act. See P.L. 107-296 § 225.

the approving official, with concurrence by the CDC, for field office requests, or OGC, for headquarters requests, as soon thereafter as practical. Given the potential effect these requests may have on First Amendment rights, it is prudent to consult with the CDC or OGC prior to approaching the service provider with the request.

Similarly, while the request to the service provider may be oral, it is preferable to make the request in writing (per the sample letter referenced above). If the request is oral, the basis for the request and the approval of the request by the service provider must be documented forthwith.

The USA Patriot Act Improvement and Reauthorization Act of 2005 created congressional reporting requirements with respect to Section 2702(b)(8) content disclosures. While there are no congressional reporting requirements under Section 2702(c)(4)for record disclosures, OGC advises that documentation of both be maintained in the investigative file. Specifically, the investigative file should contain written documentation of 1)the approval of the emergency disclosure request by the appropriate FBI official; 2)the emergency itself; and 3) the approval of the service provider. In addition, the documentation should also be kept in a control file.[7] Further guidance on this issue, as well as the issue of maintaining national security letters in the investigative file, will be forthcoming.[8]

Publicly Available Information:

In addition to NSLs, grand jury subpoenas, and emergency voluntary disclosures, there are other ways to obtain information about a telephone number. For instance, there are numerous FBI databases that include information about telephone numbers, such as [redacted]. Further, there are numerous publicly available websites (e.g., [redacted] that provide subscriber b2

[7] This accords with guidance issued by OGC on October 2, 2006, 66F-HQ-1085159, serial 71, p.4, regarding congressional reporting requirements for Section 2702 (b)(8): "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."

[8] OGC issued an EC dated August 25, 2005, 66F-HQ-1085159, serial 65, titled "Emergency Disclosure Provision for Information from Service Providers under 18 U.S.C. § 2702," which describes the emergency disclosure provision. This EC provides updated information about the provision, reflecting changes enacted in the Reauthorization Act, and supercedes the August 25, 2005 EC.

information, for a cost.[9] In addition, the FBI may access [redacted] for information about telephone numbers. b2

What You Should Not Do:

The FBI should not obtain information from a carrier by promising forthcoming legal process. Because other options are available, most notably, the emergency voluntary disclosure letter under 18 U.S.C. § 2702, there is no need to obtain telephone subscriber or toll billing information in advance of the issuance of legal process. In a genuine emergency, be it related to national security or criminal activity, the procedures set forth under 18 U.S.C. § 2702 should suffice.

Conclusion:

Investigators must follow the direction set forth above as to the techniques available to obtain telephone subscriber or toll billing records and must immediately cease the practice of obtaining information upon the promise of a forthcoming legal process. Investigators must also follow the directions set forth above with respect to use of the 18 U.S.C. § 2702 emergency disclosure provision.

Any questions concerning this guidance may be directed to Associate General Counsel [redacted] at [redacted] b6 b7C b2

[9] Public websites that have subscriber information may be accessed by investigators, provided that there is no reason to believe that the information was obtained illegally. Public websites that have information concerning toll billing records should be regarded with suspicion, as that information is generally not legally available from providers.

LEAD(s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

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

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

b6
b7C

NSLs

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 01/03/2007

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

Counterterrorism — AD Billy
DADs
Section Chiefs

Counterintelligence — AD Bereznay
DADs
Section Chiefs

Cyber — AD Finch
DADs
Section Chiefs

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

b6
b7C
b2

Approved By: Caproni Valerie E
Thomas Julie F

Drafted By: [redacted]

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

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 [redacted] 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,

b2

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. If uploaded into a database without review, 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]

b6
b7C
b2

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

1- Ms. Caproni
1- Ms. Thomas
1- [redacted] b6 b7C

[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.

This page is UNCLAS.

(Rev. 01-31-2003)

NSLs infra

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 11/16/2006

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

From: Office of the General Counsel
National Security Law Branch
Contact: National Security Law Branch, (202) 324-[redacted]

Approved By: Pistole John S
Hulon Willie T
Caproni Valerie E
Thomas Julie F

b2
b6 **Drafted By:** [redacted]
b7C

Case ID #: (U) 278-HQ-C1229736

Title: (U) REVISED PROCEDURES FOR THE SUBMISSION OF REPORTS OF POTENTIAL INTELLIGENCE OVERSIGHT BOARD MATTERS

Synopsis: (U) To provide legal guidance to all divisions regarding changes to the requirements and procedures to report conduct that may be unlawful or contrary to Executive Order or Presidential Directive (potential IOB matters). This electronic communication (EC) supersedes all previous oral and written guidance relating to reporting potential IOB matters.

(U) **~~Derived From~~: G-3**
~~Declassify On~~: X25-1

Details: (U) The President, by Executive Order 12334, dated 12/04/1981, established the President's Intelligence Oversight Board (PIOB). On 09/13/1993, by Executive Order 12863, the President renamed it the Intelligence Oversight Board (IOB) and established the Board as a standing committee of the President's Foreign Intelligence Advisory Board. Among its responsibilities, the IOB has been given authority to review the FBI's practices and procedures relating to foreign intelligence and foreign counterintelligence collection.

~~SECRET~~

This page is UNCLAS.

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE **Date:** 3/20/2006

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

Counterterrorism — AD Hulon;
DADs;
Section Chiefs

Counterintelligence — Acting AD Bereznay;
DADs;
Section Chiefs

Cyber — AD Reigel
DADs
Section Chiefs

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

Approved By: [redacted]
Caproni Valerie E

Drafted By: [redacted]

b6
b7C
b2

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

Title: LEGAL ADVICE AND OPINIONS;
SERVICE OF NATIONAL SECURITY LETTERS

Synopsis: Provides revised guidance on the service of National Security Letters (NSLs) by facsimile, as a follow-up to EC dated 6/29/2005 concerning expansion of approved methods of delivering NSLs. Specifically, the use of a non-secure fax is now an acceptable method of service of an NSL by the FBI.

Reference: 319X-HQ-A1487720-OGC, Serial 27

Details:

BACKGROUND:

The FBI issues NSLs pursuant to numerous statutes, including the Fair Credit Reporting Act, 15 U.S.C. §§ 1681u and 1681v, the Electronic Communications Privacy Act, 18 U.S.C. § 2709, and the Right to Financial Privacy Act, 12 U.S.C. § 3414. The NSLs are not classified. Nor is the information that is returned in response to an NSL (NSL return information). However, the documents that are transmitted to the receiving

entity and returned to the FBI do contain sensitive information. For that reason, the Office of the General Counsel (OGC) had opined in the past that NSLs should be personally served upon or secure faxed to the recipient and responsive information should be personally delivered or secure faxed to the FBI. However, by EC dated 6/29/2005,[1] the Security Division and OGC issued additional guidance which allowed for the delivery of NSLs via a controlled reputable delivery service such as Federal Express or the U.S. Postal Service's restricted delivery service, and allowed for the delivery of NSL return information by any reputable delivery service. The restrictions as to the requirement of secure fax transmissions remained in place.

At the time of issuance of that guidance, the Security Division and OGC represented that they would address the issue of the service of NSLs to the recipient and return of responsive information to the FBI by fax machines through future guidance.

While the secure faxing of NSLs and NSL return material continues to provide the most security for the information, OGC and the Security Division have continued to reexamine this issue. We recognize that the requirement of secure faxing of NSLs and NSL return information raises issues of efficiency, and sometimes potential harm to an investigation, as did the requirement of personal delivery. **Therefore, we have concluded that use of non-secure fax is permissible by the FBI in its service of an NSL upon the recipient.** (The same is not true of faxing of NSL return information. See below.)

However, there are conditions that attach to use of a non-secure fax to transmit an NSL to a recipient. A supervisor must approve the non-secure fax transmission. The FBI employee must call and verify that the intended person is waiting at the fax machine for the transmission. After the fax has been completed, the FBI employee must immediately call and confirm that the fax has been received. For each such non-secure fax transmission, there must be written documentation reflecting the supervisor's approval and the facts set forth above, including the time and date of the transmission, and the name of the recipient party.

The Security Division has not approved the faxing of NSL return information via non-secure fax because of the FBI's inability to hold the recipient's employees accountable for a similarly responsible process of fax transmission at their end.

---

[1] 319X-HQ-A1487720-OGC, serial 27

To: All Field Offices From: Security Division;
General Counsel

Re: 319X-HQ-A1487720-OGC 3/20/2006

CONCLUSION

This guidance provides the outer parameters of acceptable methods or service at the present time. Obviously, headquarters and field offices may choose to continue to use secure fax and personal service, as a general policy matter or as applied to individual situations, rather than controlled delivery services and non-secure fax. As with any system designed to protect security, it is the responsibility of FBI employees, in consultation with their supervisors and the Security Division, to exercise their discretion in such a manner as to assure that the method they have chosen for service adequately protects the sensitivity of the information contained in the NSL and the return information.

Any questions regarding this communication may be directed to Assistant General Counsel [redacted] at [redacted]

b6
b7C
b2

To: All Field Offices From: Security Division;
General Counsel

Re: 319X-HQ-A1487720-OGC 3/20/2006

LEAD(s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

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

1 - Mr. Phalen
1 - Ms. Caproni
1 - Ms. Thomas
1 - [redacted] b6 b7C
1 - [redacted]

♦♦

(Rev. 03-08-2006)

FEDERAL BUREAU OF INVESTIGATION

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

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

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

b6 b7C b2

Approved By: Mueller Robert S III

Drafted By: [redacted]

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

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

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

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

Specifically, the USAPA IRA provides, with respect to each of the NSL statutes set forth above, that a non-disclosure requirement attaches to the NSL "[i]f the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by

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

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

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

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

---

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

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

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

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

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

1. The Deputy Director;

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

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

---

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

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

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

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

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

7. The SACs in all other field divisions.

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

---

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

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

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

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

LEAD:

Set Lead 1: (adm)

ALL RECEIVING OFFICES

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

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/27/2005

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

Counterterrorism
AD Hulon;
DADs;
Section Chiefs

Counterintelligence
AD Szady;
DADs;
Section Chiefs

Cyber
Special Assistant AD Iannarelli
DADs
Section Chiefs

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

Approved By: Caproni Valerie E
Thomas Julie F

Drafted By: [redacted]

b6
b7C
b2

Case ID #: 319X-HQ-A1487220-OGC

Title: LEGAL ADVICE AND OPINIONS;
NSL MATTER

Synopsis: Provides guidance to field offices concerning a change to National Security Letters (NSLs) to allow for return date.

Details: This electronic communication (EC) provides guidance with respect to the modification of all NSLs to allow for a return date by which the information must be provided to the FBI.

Return Date

It has come to the attention of the Office of the General Counsel (OGC) that information sought through NSLs is often provided in a less than timely fashion by the recipient of the NSL. This compares to the generally timely provision of information in response to a grand jury subpoena. A grand jury subpoena generally has a specified date upon which the custodian of records is due to appear before the grand jury with the records that are sought by the

subpoena. Further, the grand jury subpoena often includes a date by which the custodian of records can provide the information in advance of the grand jury date in order to obviate a need for a grand jury appearance. Either way, there is a date certain by which grand jury information must be provided. Until now, the NSL form used by the FBI has not contained such information. It therefore appears to the recipient that there is no time frame by which he must produce the information, and the result is that he does not give it any tasking priority.

Although there is no statutory provision for a return date on an NSL, there does not appear to be any legal impediment to providing for such a date. Concluding that the FBI has the discretion to impose a date is comparable to the conclusion that a prosecutor has discretion to obviate a live appearance in the grand jury if the custodian produces the records by a date certain.

Further, it would be anomalous to compel production of records, as the NSL statutes do, while not allowing for specifying a date by which the records have to be produced. If "shall" is to have any meaning, it can only have meaning if there is not an endless time period by which the compelled act is required.[1]

Thus, OGC opines that an NSL may contain a return date by which the information must be provided. The return date must be reasonable and not oppressive to the recipient, in light of the nature of the request.[2] The return date should also account for how quickly the information is needed. The actual amount of time, b5

[redacted]

---

[1] The Electronic Communications Privacy Act, 18 U.S.C. § 2709, provides that the recipient "Shall comply" with a request under the statute. The Right to Financial Privacy Act, 12 U.S.C. § 3414(a)(5)(A), provides that the recipient "shall comply" with a request under the statute. The Fair Credit Reporting Act, 15 U.S.C. § 1681u, provides that the recipient "shall furnish" certain information upon request. The Fair Credit Reporting Act, 15 U.S.C. § 1681v, provides that the recipient "shall furnish" a full credit report upon request.

[2] This language tracks the language of the Fed.R.Crim.P., Rule 17(a)(2), with respect to grand jury subpoenas, whereby a motion to quash may be made if compliance with the request is unreasonable or oppressive. [redacted] b5

[redacted]

b5

[redacted] We suggest that, as a practical matter, the date be stated in terms of time that has elapsed since the NSL was served upon the recipient, rather than stating a specific date by which the information is due, in order to account for a situation in which NSL service is delayed beyond expectations.[3]

OGC will update its model NSLs to reflect the above, but until it does so, we suggest that the return date be inserted into the second to the last paragraph of the form NSL, so it would now read: "You are requested to provide records responsive to this request personally to a representative of the **[DELIVERING DIVISION]** of the FBI within [xxxx] business days of receipt of this request."

Inquiries about this guidance should be directed to Assistant General Counsel [redacted]

b6
b7C
b2

[3] Absent extraordinary circumstances, OGC suggests [redacted]

b5

To: All Field Offices From: Office of the General Counsel
Re: 319X-HQ-A1487720-OGC , 05/27/2005

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

Take action consistent with this guidance.

♦♦
1- V. Caproni
1- J. Thomas
1-
1-
1-
1-
1-

b6
b7C

[redacted] (OGC) (FBI) b6 b7C

From: [redacted] OGC) (FBI)
Sent: Thursday, October 12, 2006 3:16 PM
To: FBI_ALL CDCs
Subject: CLARIFICATION Re "From DGC Julie Thomas: NSLs - Congressional Reporting Requirements"

Importance: High

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

TO: ALL CDCs

Soon after we sent our 5 October "ALL CDC" e-mail, below, it became readily apparent that further clarification would be needed. We apologize. In this e-mail, we hope to provide the clarification.

It is NOT mandatory to send to NSLB the hard copies of ***all*** NSLs and their ECs. Hard copies are required ***only*** when the case has been deemed either SENSITIVE or RESTRICTED, in which instance the case has not been uploaded in ACS or it has been serialized in ACS without text. In such cases, we do need the hard copies to retrieve the required reporting information.

So, by way of review, exactly what do we need?

Unless the case is either SENSITIVE or RESTRICTED, **don't send** hard copies.

If the case is either SENSITIVE or RESTRICTED, then **do send** to NSLB the hard copies of the NSL and its accompanying EC. In the EC's Administrative Section, please note SENSITIVE or RESTRICTED in bold and "do not upload." Those notations will alert NSLB personnel that the Congressionally required information will not be electronically available and that they will have to retrieve the information from the hard copy. (We realize that, in some instances, there may be a case which the field will serialize but not provide the text. In that instance, that fact should be stated in bold in the EC's Administrative Section so as to alert NSLB personnel that the reporting information must be retrieved from the hard copies. Also, since the serial number would be available for such a case, please write it on the EC.)

Thank you again for your attention to this very important matter.

[redacted] b6 b7C
Assistant General Counsel
OGC / NSLB / NSLPTU

-----Original Message-----
b6 **From:** [redacted] (OGC) (FBI)
b7C **Sent:** Thursday, October 05, 2006 4:29 PM
To: FBI_ALL CDCs
Subject: From DGC Julie Thomas: NSLs - Congressional Reporting Requirements
Importance: High

): ALL CDCs

We request your help in addressing a NSL-related issue that has begun to cause NSLB a very significant problem in satisfying our strict Congressional reporting requirements.

As you know, the field submits hard copies of NSLs and their accompanying ECs to NSLB. When submitting each EC, the serial to the case file number must be recorded on the EC. **That is the rule, and there is only one exception to it:** If the case is either SENSITIVE or RESTRICTED, then that fact should be stated in bold in the Administrative Section with an accompanying note that the case should not be uploaded.

Lately, we have received numerous ECs not following the above rule. The result is an extremely adverse impact on our ability to ensure accurate reporting in satisfaction of the Congressional requirements. Please assist us by ensuring that each EC complies with the above guidance.

Thank you for your attention to this very important matter. It's truly appreciated.

Julie F. Thomas
Deputy General Counsel
National Security Law Branch

[redacted] (OGC) (FBI)

Sent: [redacted] (OGC) (FBI)
Thursday, October 05, 2006 4:03 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] OGC) (FBI); [redacted] (OGC) (FBI)
Subject: NSLs - Congressional Reporting Requirements

Importance: High

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

Julie --

[redacted] has brought to our attention a very significant and growing NSL-related issue that really should be addressed right away. She requested that we send an e-mail to all CDCs to do so.

The proposed e-mail, below, explains the problem and how we think it should be addressed.

[redacted] **has reviewed and approved the proposed e-mail. He asked me to forward it directly to you, recommending that you send it to all CDCs.**

Thanks!

[redacted]

TO: ALL CDCs

We request your help in addressing a NSL-related issue that has begun to cause NSLB a very significant problem in satisfying our strict Congressional reporting requirements.

As you know, the field submits hard copies of NSLs and their accompanying ECs to NSLB. When submitting each EC, the serial to the case file number must be recorded on the EC. **That is the rule, and there is only one exception to it:** If the case is either SENSITIVE or RESTRICTED, then that fact should be stated in bold in the Administrative Section with an accompanying note that the case should not be uploaded.

Lately, we have received numerous ECs not following the above rule. The result is an extremely adverse impact on our ability to ensure accurate reporting in satisfaction of the Congressional requirements. Please assist us by ensuring that each EC complies with the above guidance.

Thank you for your attention to this very important matter. It's truly appreciated.

Julie F. Thomas
Deputy General Counsel
National Security Law Branch

[redacted] (OGC) (FBI)

om: [redacted] (OGC) (FBI)
nt: Wednesday, October 04, 2006 6:10 PM
: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: Another NSL issue

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

b6 Can you craft an all CDC e-mail regarding this for Julie's review and approval?
b7C
Thanks.

[redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, October 04, 2006 6:04 PM
o: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
bject: Another NSL issue

b6
b7C

NSITIVE BUT UNCLASSIFIED
ON-RECORD

Dear all,

I have come across another NSL issue. As you are probably aware, the field sends in hard copies of all ECs and NSLs to NSLB. In so doing the serial to the case ID number should be recorded on the EC. The only reason this rule does not apply, is when the field deems their case to be a **sensitive** or **restricted**. Thus, it is serialized without the text. The field sends the EC and NSL to NSLB stating that this case is **sensitive** or **restricted** and should not to be uploaded. NSLB would then record the Congressional reporting information from the EC into the NSL database.

Here of late, I have noticed a tremendous amount of ECs that are not following this rule, resulting in additional searching and tracking of ECs in ACS to determine whether they have already been entered into the NSL database. The majority of them have. However, there is no way for me to know whether NSLB lead has been covered except to conduct a search in ACS.

In order to alleviate perhaps over reporting and to ensure that NSLB accurately fulfill Congressional reporting requirements, once again, I am asking is it feasible for someone to send an all CDC email addressing this issue, indicating that all "ECs relative to NSLs must have the serial to the case file number recorded on the EC, except when the case is **sensitive** or **restricted.** In this instance, it should be stated in **"bold"** in the administrative section this is a **sensitive** or **restricted** case and ould not be uploaded." Therefore, I would know to record data from the EC. Thank you for any ssistance in this matter.

[redacted]
Paralegal Specialist
National Security Law Branch
ffice of the General Counsel
oom 7975/ext. [redacted]

b6
b7C
b2

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

b6
b7C
[redacted](OGC) (FBI)
b2

From: [redacted]

Sent: Thursday, September 28, 2006 12:52 PM

Subject: Interim Standard Minimization Procedures for Business Record Orders [redacted]

UNCLASSIFIED
NON-RECORD

On September 5, 2006, the Attorney General filed Interim Standard Minimization Procedures with the FISA Court governing the retention and dissemination by the FBI of any tangible things, or information therein, received by the FBI in response to an order under 50 U.S.C. Section 1861 (Business Record Orders). [redacted]

b2 [redacted] or on the NSLB web site. There is a brief discussion of the procedures at the NSLB/OGC website, under "Business Record Orders". OIPR and the FBI are working on permanent SMPs.

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-01-2007 BY 65179dmh/kar/lmf

NSL's

[redacted](OGC)(FBI)

From: [redacted](OGC)(FBI) b6
Sent: Wednesday, May 18, 2005 1:40 PM b7C
To: [redacted]OGC)(FBI)
Subject: CRS Rpt for Congress - Admin Subpoenas & NSLs in Criminal & Foreign Intel Investigations

UNCLASSIFIED
NON-RECORD

-----Original Message-----
From [redacted] (OGC) (FBI) b6
Sent: Monday, May 09, 2005 2:47 PM b7C
To:

UNCLASSIFIED
NON-RECORD

Attached is a recent CRS Report titled, "**Administrative Subpoenas and National Security Letters in Criminal and Foreign Intelligence Investigations: Background and Proposed Adjustments**."

The first half of this report provides background information on administrative subpoenas and national security letters. The second half addresses several bills that have been proposed to amend existing laws in these areas. **Note that the Appendix provides the full text of all the applicable statutes re Administrative Subpoenas and National Security Letters.**

[redacted]

b6
UNCLASSIFIED b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-02-2007 BY 65179dmh/ksr/lmf

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

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

Total Deleted Page(s) ~ 98
Page 2 ~ Duplicate
Page 8 ~ Duplicate
Page 10 ~ Duplicate
Page 11 ~ Duplicate
Page 12 ~ Duplicate
Page 13 ~ Duplicate
Page 14 ~ Duplicate
Page 15 ~ Duplicate
Page 16 ~ Duplicate
Page 17 ~ Duplicate
Page 18 ~ Duplicate
Page 19 ~ Duplicate
Page 24 ~ Duplicate
Page 41 ~ Duplicate
Page 42 ~ Duplicate
Page 50 ~ Duplicate
Page 51 ~ Duplicate
Page 52 ~ Duplicate
Page 53 ~ Duplicate
Page 54 ~ Duplicate
Page 55 ~ Duplicate
Page 56 ~ Duplicate
Page 72 ~
outside the scope/CRS Report for Congress 3/17/06
Page 73 ~
outside the scope/CRS Report for Congress 3/17/06
Page 74 ~
outside the scope/CRS Report for Congress 3/17/06
Page 75 ~
outside the scope/CRS Report for Congress 3/17/06
Page 76 ~
outside the scope/CRS Report for Congress 3/17/06
Page 77 ~
outside the scope/CRS Report for Congress 3/17/06
Page 78 ~
outside the scope/CRS Report for Congress 3/17/06
Page 79 ~
outside the scope/CRS Report for Congress 3/17/06
Page 80 ~
outside the scope/CRS Report for Congress 3/17/06
Page 81 ~
outside the scope/CRS Report for Congress 3/17/06
Page 82 ~
outside the scope/CRS Report for Congress 3/17/06

Page 83 ~
outside the scope/CRS Report for Congress 3/17/06
Page 84 ~
outside the scope/CRS Report for Congress 3/17/06
Page 85 ~
outside the scope/CRS Report for Congress 3/17/06
Page 86 ~
outside the scope/CRS Report for Congress 3/17/06
Page 87 ~
outside the scope/CRS Report for Congress 3/17/06
Page 88 ~
outside the scope/CRS Report for Congress 3/17/06
Page 89 ~
outside the scope/CRS Report for Congress 3/17/06
Page 90 ~
outside the scope/CRS Report for Congress 3/17/06
Page 91 ~
outside the scope/CRS Report for Congress 3/17/06
Page 92 ~
outside the scope/CRS Report for Congress 3/17/06
Page 93 ~
outside the scope/CRS Report for Congress 3/17/06
Page 94 ~
outside the scope/CRS Report for Congress 3/17/06
Page 95 ~
outside the scope/CRS Report for Congress 3/17/06
Page 96 ~
outside the scope/CRS Report for Congress 3/17/06
Page 97 ~
outside the scope/CRS Report for Congress 3/17/06
Page 98 ~
outside the scope/CRS Report for Congress 3/17/06
Page 99 ~
outside the scope/CRS Report for Congress 3/17/06
Page 100 ~
outside the scope/CRS Report for Congress 3/17/06
Page 101 ~
outside the scope/CRS Report for Congress 3/17/06
Page 103 ~ Duplicate
Page 104 ~ Duplicate
Page 105 ~ Duplicate
Page 106 ~ Duplicate
Page 107 ~ Duplicate
Page 108 ~ Duplicate
Page 109 ~ Duplicate
Page 110 ~ Duplicate
Page 111 ~
outside the scope/CRS Report for Congress 4/15/05
Page 112 ~
outside the scope/4-15-05 CRS Report
Page 113 ~

outside the scope/4-15-05 CRS Report
Page 114 ~
outside the scope/4-15-05 CRS Report
Page 115 ~
outside the scope/4-15-05 CRS Report
Page 116 ~
outside the scope/4/15/06 CRS Report
Page 117 ~ Duplicate
Page 118 ~ Duplicate
Page 119 ~ Duplicate
Page 120 ~ Duplicate
Page 121 ~ Duplicate
Page 122 ~ Duplicate
Page 123 ~ Duplicate
Page 124 ~ Duplicate
Page 125 ~ Duplicate
Page 126 ~ Duplicate
Page 127 ~ Duplicate
Page 128 ~ Duplicate
Page 129 ~ Duplicate
Page 130 ~ Duplicate
Page 131 ~ Duplicate
Page 132 ~ Duplicate
Page 133 ~ Duplicate
Page 134 ~ Duplicate
Page 135 ~ Duplicate
Page 136 ~ Duplicate
Page 137 ~ Duplicate
Page 138 ~ Duplicate
Page 139 ~ Duplicate
Page 140 ~ Duplicate
Page 141 ~ Duplicate
Page 142 ~ Duplicate
Page 143 ~ Duplicate
Page 144 ~ Duplicate
Page 145 ~ Duplicate
Page 146 ~ Duplicate
Page 147 ~ Duplicate
Page 148 ~ Duplicate