(Rev. 01-31-2003)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/01/2007

To: All Divisions **Attn:** Manuals Desk
Corporate Policy Office
ADIC
SAC
ASAC
CDC

b2
b6
b7C

From: General Counsel
National Security Law Policy and Training Unit
Contact: [redacted] 202-324-[redacted]

Approved By: Caproni Valerie E
Kelley Patrick W
Thomas Julie F

DATE: 06-12-2007
CLASSIFIED BY 65179/DMH/KSR/RW
REASON: 1.4 (c)
DECLASSIFY ON: 06-12-2032

1081084

Drafted By: [redacted]: bls

b6
b7C

Case ID #: (U) 319X-HQ-A1487720-OGC (Pending)
(U) 319W-HQ-A1487699

Title: (U) COMPREHENSIVE GUIDANCE ON
NATIONAL SECURITY LETTERS

Synopsis: (U) To provide comprehensive guidance on the use, requirements, and reporting of National Security Letters.

(U) ~~**Derived From : G-3**~~
~~**Declassify On: 03/07/2032**~~

Administrative: (U) Where noted, the ECs cited in this EC are available on the NSLB NSL website.

Enclosure(s): (U) NSL Review Checklist

Details: (U) National Security Letters (NSLs) are investigative tools that allow the FBI to obtain certain limited types of information without court authorization. NSLs can be used early in a national security investigation to develop leads and to determine a subject's associates and financial dealings. Just as

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

critical, NSLs can be used to remove individuals from suspicion. The USA PATRIOT Act of 2001 changed the standard for obtaining an NSL and altered the FBI approval levels. Subsequently, NSLs have become increasingly important investigative tools in national security cases. To ensure NSLs and NSL-derived information are being used properly, FBI personnel involved in preparing these letters need to be aware of the statutory and procedural restrictions on the use of NSLs. This Electronic Communication (EC) summarizes and compiles existing and new FBI NSL policies and highlights potential issues regarding NSLs. For additional details, and the most recent guidance, on NSLs, see the National Security Law Branch (NSLB) NSL website at http://ogc.fbinet.fbi/nslb/nsl/.

(U) This guidance is effective immediately and supercedes all prior conflicting guidance. The EC summarizes, and supercedes where conflicting, policy contained in the National Foreign Intelligence Policy Manual and in ECs 319X-HQ-A1487720-OGC Serials 20, 24, 210, 213, 222, 326, 329, 331.

(U) This EC has been coordinated with the National Security Branch.

(U) Supervisors should monitor compliance with the issues and policies described in this EC. SACs should require personnel involved in the NSL process to review this document and to certify such review. A Virtual Academy Course will be available in the future and will be mandatory for all personnel involved in the NSL process.

(U) Types of Information Acquired from NSLs

(U) NSLs can be used to acquire only specific types of information from third parties.

(U) Telephone and Electronic Communication Records

(U) Under the Electronic Communications Privacy Act, 18 U.S.C. §2709, the FBI can obtain telephone and email subscriber records, as well as toll billing records information[1] and

[1] (U) Toll billing records information is not defined by statute. When serving an NSL requesting toll billing record information, there must be an attachment listing items the provider may consider to be toll billing records. See form NSLs and attachments on NSLB's NSL website.

~~SECRET~~

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

electronic communication transactional records[2] from telephone companies and internet service providers if the information is relevant to an international terrorism or counterintelligence investigation. **Content of communications cannot be obtained through an NSL.**

~~(S)~~ NSLs may be used to obtain transactional records; they may not be used to obtain content information. The line between the two is often unclear, particularly with respect to email account information.

(S) [redacted]

b1
b2
b7E
b5

(U) Financial Records

(U) Under the Right to Financial Privacy Act, 12 U.S.C. §3414(a)(5)(A), the FBI can obtain the records of financial institutions[3] if relevant to an international terrorism or

---

[2] (U) Electronic communication transactional information is not defined by statute. When serving an NSL requesting electronic communications transactional records, there must be an attachment listing the items the provider may consider to be electronic communication transaction records. See form NSLs and attachments on NSLB's NSL website. Further guidance will be forthcoming on the categories of information that may not be sought through an NSL for electronic communication transaction records which must be sequestered if received.

[3] (U) Title 31 U.S.C. § 5312(a)(2) lists those financial institutions that apply to 12 U.S.C. §3414 as: insured banks; commercial banks or trust companies; private bankers; an agency or branch of a foreign bank in the United States; credit unions; thrift institutions; brokers or dealers registered with the SEC; brokers or dealers in securities or commodities; investment bankers or investment companies; currency exchanges; issuers, redeemers or cashiers of travelers' checks, checks, money orders; operators of credit card systems; insurance companies; dealers in precious metals, stones, or jewels; pawnbrokers; loan or finance companies; travel agencies; licensed senders of money or any other person who engages as a business in the transmission of funds; telegraph companies; businesses engaged in vehicle sales, including automobile, airplane, and boat sales; persons involved in real estate closings and settlements; US Postal Service; agencies of US/state/local government carrying out any of foregoing; casinos (with certain restrictions); any businesses similar to the above list as determined by the

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

counterintelligence investigation. The statute allows the FBI to obtain any information or record "pertaining to a customer's relationship with the financial institution."[4] Although the definition of financial institution in 12 U.S.C. §3414 is broad, as a matter of policy, the records sought from such institutions must be financial in nature. For example, NSLs should not be used to obtain medical records from an insurance company, but only those financial records the company may possess.

(U) Credit Information

(U) Under the Fair Credit Reporting Act, 15 U.S.C. §1681u(a) and (b), the FBI can obtain a list of financial institutions and consumer identifying information from a credit reporting company if relevant to a counterintelligence or international terrorism investigation. Section 1681u (a) allows the FBI to obtain from credit reporting agency records the names of all financial institutions at which an individual maintains or has maintained an account, and, pursuant to 1681(b), the person's name, address, former addresses, place of employment, and former places of employment. Note that a combination 1681u(a) and 1681u(b) NSL, with cover EC, is now available on the NSLB website. This NSL can be used when requesting both the list of financial institutions and consumer identifying information from a credit reporting company.

(U) Full Credit Reports for International Terrorism Cases

(U) The Fair Credit Reporting Act, 15 U.S.C. §1681v, authorizes the FBI to obtain a full credit report pursuant to an NSL if necessary to the conduct of an international terrorism investigation. **Note, this provision does not authorize the FBI to obtain full credit reports sought for counterintelligence investigations, unless such investigation is related to international terrorism.**

Secretary of the Treasury; any businesses designated by the Secretary whose cash transactions have high degree of usefulness in criminal, tax or regulatory matters.

[4] (U) See 12 U.S.C. § 3401(2).

~~SECRET~~

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

(S) (S) For example, b1 b5

Standard for Issuing NSLs

(S) The standard for issuing an NSL, except under Section 1681v,[5] is **relevance 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 predicated solely on activities protected by the First Amendment of the Constitution of the United States.[6]

(S) b1 b5

(U) The standard of relevance is not exceedingly difficult to meet. Information is relevant if it tends to make a fact more or less probable.[7] In the context of NSLs, there must be a reasonable belief that the information sought via the NSL either supports or weakens facts being investigated in a case.

[5] (U) As discussed above, the 1681v NSL request for a full credit report is not available in counterintelligence investigations unless there is an international terrorism nexus.

[6] (U) Although the standard for the issuance of an NSL is generally described as relevance, the individual NSL statutes use varying language to describe the standard. 18 U.S.C. § 2709 requires that the information be "relevant to" an authorized national security investigation, while 15 U.S.C. § 1681u of FCRA and 12 U.S.C. § 3414 of RFPA require a certification that the information is "sought" for a national security investigation. Although in practice a similar determination is made, drafters and reviewers of NSLs should be aware of the differing language as the model NSLs contain the appropriate statutory language for each type of NSL.

[7] (U) Federal Rules of Evidence, Rule 401.

~~SECRET~~

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

For example, financial records believed to support a subject's assertion that he or she was in the United States at a given time are relevant to the investigation. On the other hand, phone records of a sibling of a subject of an investigation not known to be in contact with the subject would not, barring additional information, be relevant to the national security investigation.

(U) In addition to the information being relevant, the investigation of a United States person cannot be conducted solely based on activities protected by the First Amendment. For example, the FBI cannot issue an NSL for phone records of an attendee of a mosque that is attended by IT subjects solely because of that individual's attendance at the mosque. The individual's attendance at a place of worship is First Amendment protected activity on which the FBI cannot base an investigation. On the other hand, if the FBI reasonably believes that,

b2
b7E
b5

(U) The EC that requests the issuance of an NSL must provide a sufficiently detailed explanation of the predication for the investigation and the relevance of the material sought by the NSL so that a meaningful review can be conducted. As discussed below in more detail, a perfunctory recitation, for instance, that (1) the target of the NSL is the subject of an investigation, (2) he has a telephone, and (3) therefore it follows that an NSL for his telephone records is relevant to the authorized investigation will not suffice.

(U) In its report, the OIG provided the following example of information that would not be adequate to demonstrate relevance to a national security investigation. The requesting EC stated that an investigation had been opened "because the subject is in contact with the subjects of other international terrorism investigations. These subscriber and toll billing records are being requested to determine the identity of others with whom the subject communicates." Although the records regarding the target of this NSL may be relevant to a national security investigation, the lack of detail in that description does not permit reviewers to make an independent judgment of the relevance of the information to the investigation.

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

(U) It is incumbent upon the reviewers, including the CDC/ADC, to assure themselves that there is adequate factual predication for the investigation and that the information that is sought via the NSL will be relevant to the investigation.

Legal Review Required

(U) In the past, it has been the practice of CDCs to review and approve NSLs in the field and for NSLB attorneys to review NSLs at Headquarters. This EC reiterates and formalizes this practice. **Henceforth, all Field Office NSLs must be reviewed by CDCs or ADCs for legal sufficiency before being forwarded for SAC approval.** If legal review is not available at the Field Office, NSLB must review and approve. **All Headquarters NSLs must be reviewed by NSLB attorneys for legal sufficiency before being forwarded to the appropriate designated approving official.** CDCs, ADCs, and NSLB attorneys may find legal sufficiency only if they determine that the NSL meets the legal standards set forth above, namely that the information sought is relevant to an authorized national security investigation. The legal reviewer must exercise his or her independent legal judgment in order to assure that the issuance of the NSL comports with the law. If the CDC, ADC, or NSLB attorney determines that the NSL and accompanying EC are legally insufficient, the reviewer must return the document to the requesting employee for revision.

(U) In its review of the FBI's use of NSLs, the OIG noted that, on some occasions, CDCs/ADCs were reluctant to question the legal adequacy of the predication for the investigation in which the NSL was being requested. Approval of an NSL must include a review of the predication for the underlying investigation. The fact that there is no legal review required to open an investigation does not preclude - and in fact makes more important - review of the predication when an NSL is sought.

(U) As a part of their independent legal review of NSLs, CDCs, AGCs, and NSLB attorneys must determine whether other less intrusive means of obtaining the information are feasible. Where less intrusive means are feasible, the reviewer must not approve the NSL. More fulsome guidance on least intrusive methods will be forthcoming. In addition, if a non-disclosure provision is included, CDCs/ADCs must ensure the conditions for non-disclosure are met (discussed below).

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

Who May Approve an NSL

(U) Per EC dated 9 March 2006 (319X-HQ-A1487720-OGC, serial 210 or NSLB website), the Director has delegated final approval authority of NSLs to personnel no lower than SAC in the field and no lower than the DAD level in Headquarters.[8] The person who signs the NSL must certify the information sought is relevant to an authorized national security investigation.

(U) **Acting personnel in these positions cannot approve NSLs.** In cases where a permanent SAC is not present, NSLs may be approved and signed by SACs of other divisions or, alternatively, be issued by NSLB. Field Offices requesting NSLB to issue an NSL must send an EC to NSLB and must include sufficiently detailed information to allow NSLB to draft the approving EC and NSL and to make the requisite statutory finding of relevance.

(U) The factual review that must be done by SACs will overlap with the legal review that must be done by CDCs/ADCs in certifying that the NSL is relevant to an authorized national security investigation and that the investigation is not based solely on the exercise of First Amendment rights by a U.S. person. The concept of "relevance" spans factual and legal principles. Therefore, both the SAC and CDC/ADC must determine whether the NSL meets the applicable standard and whether the requirements for non-disclosure are met. The SAC's determination should be independent of that of the CDC/ADC.

(U) Before an NSL is signed, the approving authority should:

(1) ensure that the NSL has been approved by the CDC/ADC or by an NSLB attorney;

---

[8] (U) The EC specifically delegates NSL approving authority to 1) the Deputy Director; 2) the Executive Assistant Director for the National Security Branch; 3) the Assistant Executive Assistant Director for the National Security Branch; 4) the Assistant Directors and all Deputy Assistant Directors of the Counterterrorism, Counterintelligence, and Cyber Divisions; 5) the General Counsel and Deputy General Counsel for the National Security Law Branch; 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.

~~SECRET~~

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

(2) ensure that the information requested in the NSL matches in all respects the information described in the EC seeking the NSL;

(3) satisfy him or herself that, based on the information provided within the four corners of the cover EC, the information sought by the NSL is relevant to the investigation;

(4) satisfy him or herself that, based on the information provided within the four corners of the cover EC, the investigation is properly predicated (e.g., if the subject of the investigation is a U.S. Person the investigation cannot be predicated solely on First Amendment protected activities);

(5) make a determination whether there needs to be a non-disclosure requirement imposed on the recipient of the NSL (see discussion below regarding the non-disclosure certification); and

(6) satisfy him or herself that there are not less intrusive feasible means of obtaining the information sought.

NSL Approval Process

(U) All NSLs require two documents: the cover EC seeking approval of the issuance of the NSL and the NSL itself. In addition to these documents, as discussed above, if an SAC is not available for signature, field offices may send an EC to NSLB requesting the NSL.

Models on the NSLB Website

(U) Form NSLs and cover ECs, for every type of NSL permitted, as well as a general NSL checklist, are on NSLB's website. These forms are periodically modified to adjust for statutory or policy changes. Consistently utilizing the forms from the website will insure that all the basic statutory requirements have been met and that careless errors (e.g., citing the wrong statute) do not appear in the NSLs issued by the FBI. In addition to increasing the likelihood of errors, cutting and pasting from prior ECs can delete hidden codes in the EC and

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

result in leads not being set. **Therefore, all NSLs and cover ECs issued, whether in the field or from Headquarters, must use these forms as they appear on the NSLB website.**

(U) The body of the NSL should be limited to the language contained in the NSLB model NSLs. The information provided by the recipient must fall within the universe of information the FBI is authorized to obtain under the NSL. **If, in a particular circumstance, the investigator believes that the letter or attachment should be modified to request information that may not otherwise be produced or an attachment should be added to another type of NSL, he or she must contact NSLB for approval.**

Cover EC

(U) A cover EC requesting issuance of an NSL is required. Model ECs are available on the NSLB website. As discussed in more detail below, cover ECs are classified in accordance with the information contained therein.

(U) The cover EC serves five functions:

1. It documents the predication for the NSL by explaining how the information sought is relevant to an authorized investigation and that other relevant statutory requirements have been met;
2. It documents the approval of the NSL by appropriate personnel;
3. It documents whether there is a necessity for non-disclosure;
4. It contains information needed to fulfill Congressional reporting requirements for each type of NSL; and
5. It transmits the NSL to NSLB for Congressional reporting purposes, to CTD, CD, or Cyber for informational purposes, and, if personal service is required, to the requesting squad or delivering field division for service.

(U) NSL cover ECs issued from the field must contain the SAC and CDC/ADC among the approving supervisors. If the NSL is to be signed by a Headquarters DAD, the cover EC must list an NSLB attorney among the approving supervisors.

~~SECRET~~

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

Need for Adequate Detail in the NSL Cover EC

(U) SACs and reviewing attorneys (CDCs/ADCs in field offices and NSLB in headquarters) must determine whether the information sought by the NSL is relevant to a national security investigation from the facts contained in the NSL cover EC. Thus, the description of the predication for the investigation and the relevance of the requested information to the investigation must be sufficiently detailed so the reviewer can make that determination. If presented only with "bare bones" information of the existence of an investigation and a target's telephone number or bank account number, the SAC and the reviewing attorney cannot make an informed judgment that administrative and legal requirements have been fulfilled. Thus, the recitation of facts justifying the initiation and maintenance of an investigation serves to support both the SAC certification and the legal review. This does not mean that the approval EC must recite every fact that formed the predication for the investigation or every fact that explains the manner in which the information sought is relevant to the investigation. Instead, there must be sufficient detail within the four corners of the EC so that a reasonable person without independent knowledge of the investigation can fairly judge whether the underlying investigation was adequately predicated and whether the information sought is relevant.

[redacted]

b1
b5
b2
b7E

Investigative Case File Number

(U) ECs seeking approval for the issuance of an NSL must reference the investigative case file or sub-file number of the investigation to which the NSL relates. Without reference to an authorized investigation, it is difficult to assure, for

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

congressional reporting purposes and DOJ auditing purposes, that the requirements of the NSL statute were met. Thus, NSLs must no longer be issued with a reference solely to a control file created for an investigation.[9] Pursuant to guidance issued 9 March 2007(319W-HQ-A1487699-RMD, Serial 17 or NSLB website), NSLs should now be uploaded in ACS with the specific type of NSL entered as the "document type."

Non-Disclosure Certification

(U) Prior to the USA PATRIOT Improvement and Reauthorization Act of 2005(PATRIOT Act IRA), non-disclosure provisions were statutorily required for all NSLs. (See EC dated 7 March 2006, 319X-HQ-A1487720-OGC, serial 216, for additional discussion of procedural changes pursuant to PATRIOT Act IRA.) With the passage of PATRIOT Act IRA, FBI officials must make a case by case determination whether disclosure of the NSL may: endanger 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 any person. If any of these risks would be created by disclosure of the NSL, then a non-disclosure provision may be included in the NSL. Non-disclosure would be appropriate, for example, if disclosure could alert a subject of a national security investigation to the existence of the investigation. Subsequently, the subject may take action to evade future surveillance or detection. Additional examples of when non-disclosure is appropriate are available on the NSLB website. While in most situations non-disclosure will be appropriate, all reviewers should remember that certification is not automatic. The signature of the issuing official on an NSL that includes a non-disclosure order constitutes that person's certification that at least one of the reasons for non-disclosure is present.

(U) Non-disclosure is not required in all NSLs, although the statutory standard for non-disclosure will be met in most cases. **This requirement is a major change from the NSLs issued before the PATRIOT Act IRA and, accordingly, NSL drafters**

[9] (U) There is no longer a separate OGC NSL file number (the "66" file) that must be referenced in the EC.

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

must ensure they are using the most recent model cover ECs and NSLs from the NSLB NSL website.

Reporting Paragraph

(U) The FBI is required to report information about its use of NSLs to Congress. Therefore, it is crucial that the portion of the EC that addresses those reporting requirements, as set forth below, be accurate.

(U) Although United States Person (USP) status of the target of an NSL does not play a role in the approval of NSLs, such status must be documented for Congressional reporting purposes. The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG) define a United States person as "an individual who is a United States citizen or an alien lawfully admitted for permanent residence; an unincorporated association substantially composed of individuals who are United States persons; or a corporation incorporated in the United States."

~~(S)~~ As a result of the PATRIOT Act IRA, the United States Person (USP) status of the subject of all NSL requests must be reported to Congress. Prior to the change, the NSL statutes had been interpreted to simply require the USP status of the target of the investigation. The PATRIOT Act IRA requires that the FBI provide Congress with the total number of different persons about whom it has requested information through the use of NSLs and the USP status of each such person.

(S)

b1
b2
b7E
b5

(U) The cover EC authorizing and reporting the NSL may discuss more than one subject, more than one account, and more than one NSL recipient, if all of the requests are related. While all can be combined in one cover EC, the EC must break down the number of different requests that are addressed to each and every NSL recipient. For example, if there are three persons about whom information is being sought, ten accounts, and six recipients of an NSL, then the EC must state how many requests

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

are being made in the NSL to recipient 1, to recipient 2, etc. It is not sufficient to state that there are ten accounts and six recipients.

(U) Also, the cover EC must clearly identify the type of information that is being sought. NSLs that seek toll billing records information or electronic communication transactional records will include subscriber information and thus will be reported as toll billing records information or electronic communication transactional records NSLs. The reporting paragraph must be consistent and state that toll billing records information or electronic communication transactional records are being sought for x number of subjects (and list their USP status), accounts, and, if multiple recipients, the number for each recipient.

The NSL

(U) All NSLs must be addressed to the specific company point of contact (POC). Many of these contacts are listed on NSLB's NSL POC website. All NSLs must identify the statutory authority for the request, the type of records requested, and provide identifying information to assist the company in processing the request.

(U) All NSLs require a certification that the records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities[10] and that an investigation of a USP is not conducted solely on the basis of First Amendment rights.

Recent Changes in NSL Language as a Result of the PATRIOT Act IRA

(U) Recipients are now "DIRECTED" to produce the information rather than simply "requested." This language makes clear that recipients are required to produce the information. Drafters must review NSLs and NSL cover ECs to ensure that all

[10] (U) As noted above, the 1681v NSL request for a full credit report is not available in counterintelligence investigations unless there is an international terrorism nexus.

~~SECRET~~

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

the particulars match (i.e., the request in the NSL matches exactly what is sought in the cover EC). Typographical errors in the NSL may result in overcollection of information and merit reporting as a possible IOB violation. In this regard, **drafters must pay particular attention that phone numbers and account numbers are correct.**

(U) As discussed above, the non-disclosure provision may no longer automatically be included in the NSL. If the requesting party seeks to have a non-disclosure provision included in the NSL, there must be a certification that disclosure of the NSL may endanger 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 any person. The documentation of this certification must also be contained in the cover EC.

(U) If there is a non-disclosure requirement included in the NSL, the recipient may not disclose the fact of the request to anyone except those in the company that have a need to know in order to comply and to legal counsel, if necessary. Further, the NSL informs the recipient that he must convey the non-disclosure requirement to persons who have such a need to know, and that, if asked, he must inform the FBI of the names of those persons (except counsel). In addition, the NSL informs the recipient of the process by which he can challenge the non-disclosure order and the NSL itself, and provides notice that the FBI can enforce the NSL if he does not comply. The NSL also directs the recipient to provide the information to the FBI via any reputable delivery service (e.g., Federal Express, United Parcel Service) or personal delivery.

Retention of Copies

(U) Copies of signed NSLs must be retained in the investigative file, and the NSL itself must be uploaded as an NSL document into ACS. A lead in the EC must be set to both NSLB and the relevant operational unit in headquarters.

(U) Because the NSL statutes now clearly authorize an NSL recipient to challenge both production of records under the NSL and the non-disclosure provision, the service of the NSL must

~~SECRET~~

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

be documented. That documentation should be kept with the copy of the signed NSL in the investigative file.

(U) Case agents should follow up on the service of an NSL to determine whether the third party provided the requested information. If the third party does not provide the requested information in a reasonable period of time, case agents should first notify the company that the information was not received. If non-compliance continues to be an issue, contact NSLB.

Handling of NSL-Return Information

(U) Immediately upon receiving materials in response to an NSL **and before uploading the information into any database**, the case agent is responsible for ensuring that the materials are responsive to the request and that there has been no overproduction.[11] If the information is appropriately responsive, the receiving agent should ensure the information is stored in the appropriate investigative file and that receipt is documented. Relevant information properly obtained in response to a valid NSL may be uploaded to FBI databases.

(U) Any material that is not covered by the four corners of the request (including its attachment) must be handled as discussed below. Information obtained in response to an NSL that is not covered within the four corners of the NSL (including its attachment) can fall into one of two categories: it can be irrelevant information to which the FBI has no right (hereafter "Irrelevant Information") or it can be relevant information that was simply in excess of the request (hereafter "Relevant Overproduction"). Irrelevant Information is collected, for example, when a telephone company inverts numbers in a telephone number and therefore erroneously provides the FBI toll billing information concerning the wrong telephone. Relevant Overproduction occurs, for example, when the NSL seeks financial information on John Doe for a certain time period. The bank

[11] (U) If a serving office is merely passing return information to the originating office for review and uploading, and documenting delivery through an EC, that EC should not contain substantive information from the NSL response.

~~SECRET~~

~~SECRET~~

provides the information for the requested period but also provides records for an additional two months that were not requested in the NSL. Both constitute an overcollection, but they must be treated differently.

(U) If Irrelevant Information is obtained, it may not be retained or uploaded into any FBI database. It is for this reason that it is critical that all information returned in response to an NSL be reviewed **PRIOR** to uploading it into any database, including Telephone Applications. Any Irrelevant Information should be immediately sequestered with the CDC (NSLB at Headquarters) and a potential IOB prepared. NSLB will confirm whether it is Irrelevant Information and, if so, direct that it be either returned or destroyed.

(U) If Relevant Overproduction is obtained, it must be sequestered and may not be uploaded into any FBI database or utilized in any manner until another NSL has been issued to address the overproduction. Any portion of the information that was responsive to the NSL originally served may be uploaded and used immediately. A potential IOB should be prepared with regard to the Relevant Overproduction.[12]

Dissemination of NSL-Return Information

(U) As with all information acquired in the context of a national security investigation, information properly obtained through the use of an NSL may be disseminated only in accordance with the standards set forth in the NSIG. Dissemination is also subject to specific statutory limitations. The communication record NSL statute, ECPA, and the financial record NSL statute, RFPA, permit dissemination if it is in accordance with NSIG and if the information is clearly relevant to responsibilities of recipient agency. FCRA, 15 U.S.C. §1681u, the statute authorizing the collection of limited credit information, permits dissemination to other federal agencies as may be necessary for

[12] We recommend that during quarterly file reviews, squad supervisors conduct, at a minimum, spot checks of NSL return information to ensure that case agents are following these procedures.

~~SECRET~~

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

the approval or conduct of a foreign counterintelligence investigation or where the information concerns a person subject to the Uniform Code of Military Justice, as may be necessary for the conduct of a joint FCI investigation. There are no special statutory rules for dissemination of full credit reports, FCRA, 15 U.S.C. §1681v.

Use of NSL-Return Information

(U) NSL return information may generally be used as evidence in criminal proceedings with no special handling requirements. The legal process used to obtain information - be it a grand jury subpoena or an NSL - is generally not at issue at trial, inasmuch as the government usually must only establish through a custodian of records that the information is a business record kept in the ordinary course of business.

[redacted] b2 b7E b5

[redacted] b2 b5

Prohibition on Use of "Exigent Letters"

(U) Information that is subject to ECPA (telephone and communications records) may not be obtained in advance of issuance of an NSL or grand jury subpoena unless an emergency disclosure letter is provided to the telephone company or ISP. The practice of requesting and accepting such information upon the promise of issuance of legal process in the future is

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

prohibited. In the event of an emergency, information may be obtained pursuant to 18 U.S.C. §§ 2702(b)(8) and 2702 (c)(4) if the communications 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." In these circumstances, the provider must have adequate information for a determination that an emergency exists. Compliance with requests of this nature is purely voluntary. If the provider refuses to provide the requested information, the FBI cannot compel its production under 18 U.S.C. § 2702.[13] The information that may be obtained pursuant to 18 U.S.C. § 2702 includes both the content of communications (section (b)(8)) and customer records (section (c)(4)). See 319X-HQ-A1487720-OGC Serial 331 (or NSLB website) for further details as to the policy prohibiting the use of "exigent letters" and describing the use of emergency disclosure letters in accordance with 18 U.S.C. § 2702.

(U) Once an emergency disclosure letter is issued, no further legal process is required. Some providers in the field continue to insist on legal process even after voluntarily providing information pursuant to a 2702 letter. Please consult with OGC if this issue arises.

(U) The practice of requesting and accepting RFPA and FCRA protected information upon the promise of issuance of legal process in the future is also prohibited. The emergency disclosure provision of 18 U.S.C. § 2702 does not apply to RFPA- or FCRA-protected information.

Classification Issues

(U/FOUO) As a general matter, the EC requesting an NSL is classified. If information that is included in the EC has already been classified, and the EC therefore is being derivatively classified, the classification level is equal to that of the original classification of the information. If, on

[13] (U) The FBI may, however, seek the information with an NSL or grand jury subpoena, if appropriate.

~~SECRET~~

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

the other hand, the information is being originally classified based on the FBI Classification Guide, the document classification generally should be ten years, unless there are sensitive circumstances that justify classification for 25 years. Only an authorized Original Classification Authority may originally classify information. An EC providing additional information on NSL classification is forthcoming.

(U) **Although the requesting EC is generally classified, neither an NSL itself nor the material received in return from the NSL is classified.** Thus, information obtained pursuant to an NSL may be used in criminal proceedings without declassification. As noted above, issues may arise, however, [redacted] b2 b5

(S) [redacted] b1 b2 b7E

Cases Exempted from ACS Uploading

[redacted] b1 b2 b7E

~~SECRET~~

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

Potential IOBs Regarding NSLs

(U) The misuse of NSL authorities or NSL-derived information constitutes a potential IOB. For additional information on IOBs, see EC, dated 11/16/2006, 278-HQ-C1229736, serial 2570. Potential IOB violations involving NSLs include, but are not limited to:

(U) ~~(S)~~ 1) Receiving information beyond the scope of an NSL (including the attachment) is a potential IOB violation regardless of whether the overproduction occurred as a result of an error by the FBI or the NSL recipient. Examples of such overproduction include the recipient providing data on the wrong phone number or providing a full credit report when only limited data was requested. If this occurs, the field must sequester the overproduction with the Chief Division Counsel pending resolution of the potential IOB matter. As part of the adjudication process, NSLB will advise the field whether the overproduced information may be used or whether the information must be returned or be destroyed with appropriate documentation to the file.

(U) ~~(S)~~ 2) Serving an NSL that contains a substantive typographical error that results in the acquisition of data that is not relevant to an authorized investigation (e.g., numbers on telephone number transposed).

(U) ~~(S)~~ 3) Serving an NSL that requests information that is beyond the scope permissible by statute (e.g. seeking content information; seeking a full credit report during a counterintelligence investigation).

(U) ~~(S)~~ 4) Failing to meet the statutory standard for issuance of an NSL (e.g., [redacted] b1
(S) [redacted] relevance to the open investigation not demonstrated).

Reimbursement Policy for NSL-Return Information

~~SECRET~~

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

(U) An EC dated 11 April 2006 (319X-HQ-A1487720-OGC, serial 222, see NSLB NSL website) details the FBI's policy regarding reimbursement to providers of information pursuant to an NSL. Amid confusing and inconsistent practices, the policy was intended to create consistency in the way in which different field offices provide compensation to NSL recipients. The current FBI policy is to provide reimbursement only when legally required by statute, unless the request is extraordinarily burdensome.[14]

(U) Because there is no legal obligation for the FBI to compensate recipients of NSLs pursuant to ECPA (toll billing records information, subscriber, electronic communication transactional records) or FCRA Section 1681v (full credit reports in international terrorism cases), there should not be payment in connection with those NSLs. The reimbursement EC referenced above provides a form response letter to NSL recipients that request payment. See EC, 319X-HQ-A1487720-OGC, serial 222, referenced above, for additional details.

(U) Compensation is legally required for NSLs served to obtain financial information pursuant to RFPA and credit information pursuant to FCRA § 1681u. More information regarding payment schedules is available in the EC addressing reimbursement.

Questions and Additional Information

(U) For additional information, the most current NSL templates, and most current NSL cover EC templates visit the NSLB NSL website at http://ogc.fbinet.fbi/nslb/nsl/. For questions regarding NSLs, contact your NSLB operational attorney or AGC [redacted] 202-324-[redacted]

b2
b6
b7C

[14] (U) There may be situations in which lack of compensation is unduly harsh in light of the burden placed on the carrier by an NSL request. Such situations may be addressed on a case-by-case basis. This flexibility is conceptually analogous to the provision of ECPA, 18 U.S.C. § 2706, which authorizes court-ordered compensation when criminal legal process seeking telephone records is especially burdensome.

~~SECRET~~

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

(U) Disseminate to personnel involved in Counterintelligence, International Terrorism, and Cyber operational issues, and other personnel as appropriate.

Set Lead 2: (Info)

DIRECTOR'S OFFICE

AT CPO, DC

(U) This policy is provided to the CPO for tracking purposes. Read and clear.

Set Lead 3: (Action)

RECORDS MANAGEMENT

AT WASHINGTON, DC

(U) Take appropriate action to revise any superceded guidance contained in National Foreign Intelligence Policy Manual and in ECs 319X-HQ-A1487720-OGC Serials 20, 24, 210, 213, 222, 326, 329, 331.

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

~~SECRET~~

~~SECRET~~

To: All Divisions From: General Counsel
Re: (U) 319X-HQ-A1487720-OGC, 06/01/2007

1 - [redacted]
1 - [redacted]
1 - [redacted]

b6
b7C

1 - Ms. Beers

♦♦