

FBI INFO
CLASSIFIED BY: NSICG
REASON: 1.4 (C)
DECLASSIFY ON: 12-31-2041
DATE: 05-28-2019

b6 -1
b7C -1

~~SECRET//NOFORN~~

**(U) STANDARD MINIMIZATION PROCEDURES FOR FBI ELECTRONIC
SURVEILLANCE AND PHYSICAL SEARCH CONDUCTED
UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT**

~~Classified by: John P. Carlin, Assistant Attorney General for National Security
Derived from: DOJ/NSISCG-1, 1.6; FBI/NSICG INV
Declassify on: 20410516~~

~~SECRET//NOFORN~~

TABLE OF CONTENTS

I. (U) GENERAL PROVISIONS 1

II. (U) ACQUISITION 4

 A. (U) Acquisition -- Electronic Surveillance 4

 B. ~~(S//NF)~~ Acquisition -- Physical Search [redacted] (S) 5

 1. (U) Personnel Authorized to Conduct Physical Search 5

 2. (U) Conducting Physical Search 6

 a. (U) Areas of search 6

 b. (U) Manner of search 6

 i. [redacted] (S) 7

 ii. [redacted] 7

 iii. (U) Destructive Testing 7

 c. ~~(S//NF)~~ United States Person [redacted] (S) 7

 3. (U) Physical Search Involving Mail or Private Couriers 8

 4. (U) Record of Information Collected in Physical Search 8

 5. (U) Report of Physical Search 8

 C. ~~(S//NF)~~ Acquisition -- Third Parties 9

III. (U) RETENTION 9

 A. (U) General 9

 B. (U) Definitions 10

 C. (U) Additional Provisions Regarding Access, Review, and Use of FISA-acquired Information 12

b1 -1
b3 -1

b1 -1
b3 -1

b1 -1
b3 -1

- 1. (U) Review and Use of FISA-acquired Information..... 12
 - a. (U) General 12
 - b. (U) Information meeting criteria..... 12
 - c. (U) United States person identities 13
 - d. (U) Disclosure and dissemination 14
 - e. (U) Exculpatory, impeachment, and discoverable material..... 14
 - f. (U) Third-party information..... 14
 - g. (U) Sensitive information 15
- 2. (U) Procedures Regarding Access to FISA-acquired Information Retained in Electronic Form..... 16
- D. (U) Electronic and Data Storage Systems 16
 - 1. (U) Access to information and auditing requirement..... 16
 - 2. (U) Marking 17
 - 3. (U) Queries..... 17
 - 4. (U) Retention Time Limits..... 19
 - a. (U) Standard for Retention..... 19
 - b. (U) Information that has not been reviewed 19
 - c. (U) Information that has been reviewed but not identified as meeting the applicable standard..... 19
 - (U) 5. ~~(S//NF)~~ Retention of Attorney-Client Communications 20
 - (U) a. ~~(S//NF)~~ Target charged with a crime pursuant to the United States Code 20
 - (U) b. ~~(S//NF)~~ Target charged with a non-Federal crime in the United States and persons other than a target charged with a crime in the United States 22

(U) c. ~~(S//NF)~~ Privileged communications involving targets and other persons not charged with a crime in the United States 24

E. (U) Ad Hoc Systems 26

1. (U) Standard for Use 26

2. (U) Disclosure, Dissemination, Compliance, and Privilege 26

3. (U) Access to and Identification of FISA-Acquired Information 26

4. (U) Retention of FISA-Acquired Information 27

5. (U) Analysis and Queries of Raw FISA-Acquired Information 28

(U) 6. ~~(S//NF)~~ Procedures for Retention of Attorney-Client Communications 29

(U) a. ~~(S//NF)~~ Target charged with a crime pursuant to the United States Code, target charged with a non-Federal crime in the United States and persons other than a target charged with a crime in the United States 29

(U) b. ~~(S//NF)~~ Other attorney-client privileged communications 30

F. (U) Special Purpose Systems 31

(S) [Redacted Section] 31
31
32
32
33
34
34
34
35

b1 -1
b3 -1
b7E -2

H. (U) Additional Procedures for Retention, Use, and Disclosure 36

1. (U) Law Enforcement 36

2. (U) Identities 36

3. (U) Prosecutors 36

I. (U) Other Time Limits for Retention 39

 1. (U) Retention on media 39

 2. (U) Audio and video 40

 3. (U) Backup and evidence copies in FBI systems 40

 4. (U) Information retained in connection with litigation matters 41

(U) 5. ~~(S//NF)~~ Encrypted Information 41

 6. (U) Retention in other form 42

IV. (U) DISSEMINATION AND DISCLOSURE 42

 A. (U) Dissemination of Foreign Intelligence Information to
 Federal, State, Local and Tribal Officials and Agencies 42

 1. (U) Foreign Intelligence Information as defined in 50 U.S.C. § 1801(e)(1) 43

 2. (U) Foreign Intelligence Information as defined in 50 U.S.C. § 1801(e)(2) 43

 B. (U) Dissemination of Evidence of a Crime to Federal, State, Local, and Tribal Officials,
 and the National Center for Missing and Exploited Children (NCMEC) 43

 C. (U) Dissemination to Foreign Governments 44

 D. (U) Disclosure of Raw FISA-Acquired Information for Technical or
 Linguistic Assistance 46

(S) E. ~~(S//NF)~~ Disclosure Under Docket Number 48

(U) F. (U) Dissemination of Foreign Intelligence Information for Terrorist Screening 49

 G. (U) Disclosure to the National Counterterrorism Center (NCTC) of Unminimized
 Information Acquired in Cases Related to Terrorism or Counterterrorism 49

b1 -1
b3 -1
b7E -2

H. (U) Dissemination of Foreign Intelligence Information or Evidence of a Crime Involving Computer Intrusions or Attacks to Private Entities and Individuals 50

I. (U) Dissemination to Private Entities and Individuals of Foreign Intelligence Information or Evidence of a Crime Involving a Matter of Serious Harm..... 51

V. (U) COMPLIANCE 52

 A. (U) Oversight 52

 B. (U) Training53

 C. (U) Minimization Briefings 53

VI. (U) INTERPRETATION 54

VII. (U) REVIEW OF PROCEDURES 54

I. (U) GENERAL PROVISIONS

A. (U) In accordance with 50 U.S.C. §§ 1801(h) and 1821(4), these procedures govern the acquisition, retention, and dissemination of nonpublicly available information concerning unconsenting United States persons that the Federal Bureau of Investigation (FBI) obtains pursuant to orders issued by the Foreign Intelligence Surveillance Court (FISC or the Court) or emergency authorizations by the Attorney General under the Foreign Intelligence Surveillance Act of 1978, as amended (FISA), 50 U.S.C. §§ 1801-1811 and 1821-1829. Except where indicated, these procedures apply to FISA-acquired information in any form. For the purpose of these procedures, the term "applicable FISA authority" refers to both FISC-ordered and Attorney General authorized electronic surveillance or physical search conducted in a particular case pursuant to FISA. The Attorney General has adopted these procedures after concluding that they meet the requirements of 50 U.S.C. §§ 1801(h) and 1821(4) because they are specific procedures that are reasonably designed in light of the purpose and technique of the particular surveillance or physical search to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information and otherwise comport with the statutory definition of minimization procedures. In accordance with 50 U.S.C. § 403-1(f)(6), the Director of National Intelligence (DNI) has provided assistance to the Attorney General with respect to the dissemination procedures set forth herein so that FISA-acquired information may be used efficiently and effectively for foreign intelligence purposes.

B. (U) Pursuant to 50 U.S.C. §§ 1806(a) and 1825(a), no information acquired pursuant to FISA may be used or disclosed by Federal officers or employees except for lawful purposes. Information acquired from electronic surveillance or physical search conducted under FISA concerning United States persons may be used and disclosed by Federal officers and employees without the consent of the United States persons only in accordance with these minimization procedures and any modified or supplemental minimization procedures that may apply. These procedures do not apply to publicly available information concerning United States persons, nor do they apply to information that is acquired, retained, or disseminated with a United States person's consent. In addition, except for the provisions set forth below regarding attorney-client

b3 -1
b7E -1

C. (U) These procedures adopt the definitions set forth in 50 U.S.C. § 1801, including those for the terms "foreign intelligence information" and "United States person." For purposes of these procedures, if an individual is known to be located in the United States, or if it is not known whether the individual is located in or outside of the United States, he or she should be presumed to be a United States person unless the individual is identified as an alien who has not been admitted for permanent residence or circumstances give rise to the reasonable belief that the individual is not a United States person. If an individual is known or believed to be located outside the United States, he or she should be presumed to be a non-United States person unless the individual is identified as a United States person or circumstances give rise to the reasonable

belief that the individual is a United States person. In an on-line operation, if it is not known whether an individual is located in or outside of the United States, he or she should be presumed to be a non-United States person unless the individual is identified as a United States person or circumstances give rise to the reasonable belief that the individual is a United States person.

D. (U) If FBI personnel, which, for the purposes of these procedures, includes all contractors and others authorized to work under the direction and control of the FBI on FISA related matters, encounter a situation that they believe requires them to act inconsistently with these procedures in order to protect the national security of the United States, enforce the criminal law, or protect life or property from serious harm, those personnel immediately should contact FBI Headquarters and the Office of Intelligence of the National Security Division of the Department of Justice (NSD) to request that these procedures be modified. The United States may obtain modifications to these procedures with the approval of the Attorney General and a determination by the FISC that the modified procedures meet the definition of minimization procedures under sections 1801(h) and/or 1821(4) of FISA.

E. (U) If, in order to protect against an immediate threat to human life, the FBI determines that it must take action in apparent departure from these procedures and that it is not feasible to obtain a timely modification of these procedures from the FISC, the FBI shall report that activity promptly to the NSD, which shall notify the FISC promptly of such activity.

F. (U) Nothing in these procedures shall restrict the FBI's performance of lawful oversight functions of its personnel or systems, or lawful oversight functions of the NSD or the Department of Justice Office of the Inspector General. Similarly, and notwithstanding any other

section in these procedures, the FBI may use information acquired pursuant to FISA to conduct security assessments of its systems in order to ensure that FBI systems have not been compromised. These security assessments may include, but are not limited to, the temporary retention of FISA-acquired information in a separate system for a period not to exceed one year. While retained in such a system for security assessments, such FISA-acquired information may not be accessed for any other purpose. Any information retained for this purpose may be disseminated only in accordance with the applicable provisions of these procedures.

II. (U) ACQUISITION

A. (U) Acquisition – Electronic Surveillance.

1. (U) Prior to initiating electronic surveillance, the FBI shall verify that the facility or place at which it will direct surveillance is the facility or place specified in the applicable FISA authority. The FBI is under a continuing obligation to verify that the authorized target of the surveillance uses or is about to use the facility or place at which the surveillance is directed during the authorized period of surveillance. The FBI shall terminate electronic surveillance of a facility or place as soon as it determines that the authorized target of the electronic surveillance no longer uses, nor is about to use, the facility or place, and shall promptly notify the NSD of such termination.

(U) 2. ~~(S/NF)~~ When conducting electronic surveillance of a facility or place pursuant to the applicable FISA authority, the FBI may acquire, using the means and to the extent approved by the court or authorized by the Attorney General for that facility or place, (S)

b1 -1
b3 -1
b7E -1, 2

b1 -1
b3 -1
b7E -1, 2

[Redacted]

(S)

(U) 3. ~~(S//NF)~~ Notwithstanding Section II.A.2, the FBI shall, to the extent reasonably feasible: (a) use means of surveillance that are designed to limit the acquisition of nonpublicly available information or communications of or concerning unconsenting United States persons that are not foreign intelligence information relative to a target of the surveillance; and

[Redacted]

(S)

[Redacted]

b1 -1
b3 -1
b7E -1, 2

(U) B. ~~(S//NF)~~ Acquisition - Physical Search

[Redacted]

(S)

b1 -1
b3 -1
b7E -1, 2

1. (U) Personnel Authorized to Conduct Physical Search.

(U) ~~(S//NF)~~ Physical search shall be conducted only by: (i) appropriately authorized and trained personnel of the FBI, not including contractors

[Redacted]

[Redacted]

(S)

b1 -1
b3 -1
b7E -1, 2

[Redacted]

Pursuant to 50 U.S.C. § 1824(c)(2)(B)-

(S)

(D), other person may assist in the physical search as specified in the applicable FISA authority.

b1 -1
b3 -1
b7E -1, 2

2. (U) Conducting Physical Search.

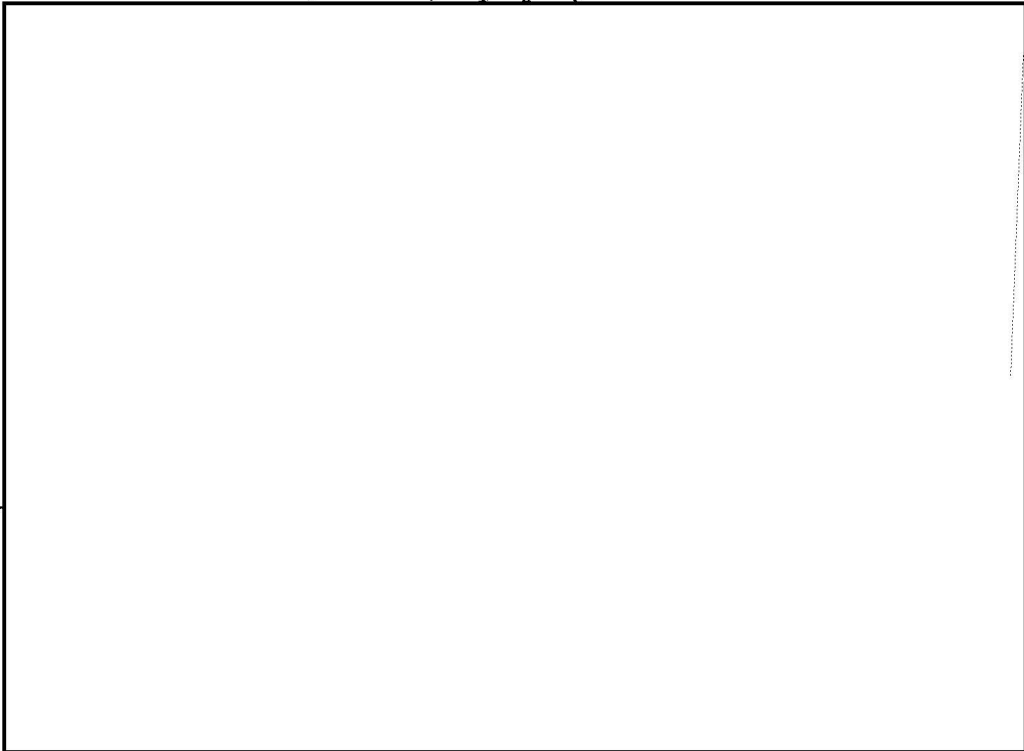
(U) Prior to initiating physical search, the FBI shall verify that the premises or property at which it will conduct physical search is the premises or property specified in the applicable FISA authority. The FBI shall conduct physical search with the minimum intrusion necessary to acquire the foreign intelligence information sought. Personnel conducting physical search shall exercise reasonable judgment in determining whether the information, material, or property revealed through the search reasonably appears to be foreign intelligence information relating to a target of the search or evidence of a crime. The FBI shall conduct the search in accordance with the applicable FISA authority.

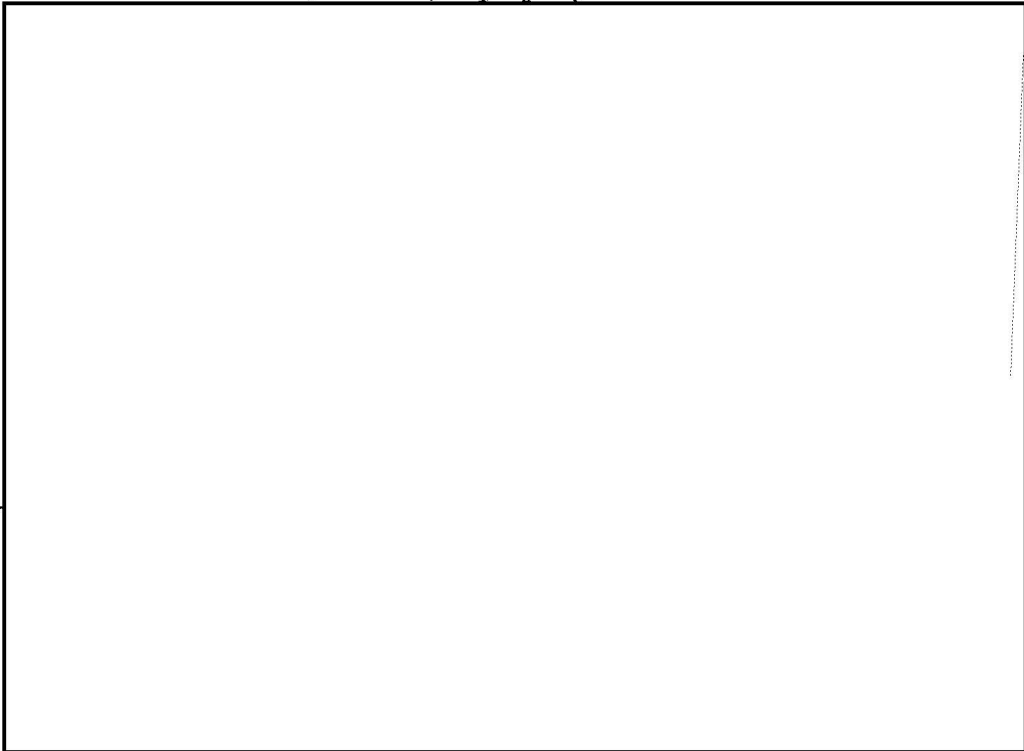
a. (U) Areas of search. For physical search of premises or property, after conducting any necessary protective sweep, the FBI shall, where reasonably feasible, limit search areas to locations within premises or property where the FBI reasonably expects that: (i) foreign intelligence information may be stored or concealed by the target; or (ii) foreign intelligence information related to the target or the activities of the target may be found.

b. (U) Manner of Search. The FBI may conduct physical search using the methods most suitable for acquiring the foreign intelligence information sought in light of the particular circumstances of the search. When conducting a physical search of electronic data, the FBI may acquire all information, communications, or data relating to the target in accordance with the applicable FISA authority. Methods used to conduct physical search may include:

inspection; examination; reproduction; temporary removal; marking for identification; testing; alteration; substitution; or seizure of information, material, or property.

b1 -1
b3 -1
b7E -1, 2

i. 

ii. 

(S)

iii. (U) Destructive Testing. The FBI may conduct destructive testing of material discovered in a physical search only when such testing is provided for in the applicable FISA authority or in case of emergency when reasonably necessary to protect against immediate threat to public safety.

(U)

c. ~~(S//NF)~~ United States Person Information, Material, or Property

b1 -1
b3 -1
b7E -1, 2



(S)

b1 -1
b3 -1
b7E -1,2

[Redacted]

(S)

3. (U) Physical Search Involving Mail or Private Couriers.

a.

[Redacted]

(S)

[Redacted]

b1 -1
b3 -1
b7E -1,2

b.

[Redacted]

(S)

[Redacted]

4. (U) Record of Information Collected in Physical Search.

(U) The FBI shall keep records identifying all information, material, or property acquired during a physical search.

5. (U) Report of Physical Search.

(U) ~~(S/NF)~~ Within seven business days following the execution of a physical search, or receiving notice that a search has been executed, and for which the FISC ordered that a search return be filed, the FBI shall notify the NSD of the date the search took place. The preceding requirement shall not apply [Redacted]

b1 -1
b3 -1
b7E -1,2

(S)

(U) C. ~~(S//NF)~~ Acquisition -- Third Parties.

(U) ~~(S//NF)~~ "Third-party information" is: (a) nonpublicly available information of or concerning an unconsenting United States person who is not the authorized target of the particular FISA collection

[Redacted]

(S)

[Redacted]

b1 -1
b3 -1
b7E -1, 2

III. (U) RETENTION

A. (U) **General.** Except where indicated below, these retention provisions apply to FISA-acquired information FBI retains in any form.

1. (U) Access to FISA-acquired information retained in any form. The FBI must retain all FISA-acquired information under appropriately secure conditions that limit access to such information only to individuals who require access in order to perform their official duties or assist in a lawful and authorized governmental function. FBI personnel with access to raw FISA-

acquired information must receive training on these minimization procedures before receiving access to raw FISA-acquired information. Access to FISA-acquired information contained within different systems shall be appropriately restricted, even when the systems are not physically separated. Such secure conditions and limitations on access may be effected by physical separation, logical partition, or a combination of both.

b1 -1
b3 -1
b7E -1, 2

2

(S)

B. (U) Definitions. For purposes of these procedures:

- (U) 1. ~~(S//NF)~~ "FISA-acquired information" means all information, communications, material, or property that the FBI acquires from electronic surveillance or physical search conducted pursuant to FISA.
- (U) 2. ~~(S//NF)~~ "Raw FISA-acquired information" is FISA-acquired information that (a) is in the same or substantially same format as when the FBI acquired it, or (b) has been processed only as necessary to render it into a form in which it can be evaluated in accordance with these procedures. Raw FISA-acquired information, however, does not include information the FBI has determined, in accordance with these procedures, to reasonably appear to be foreign intelligence

b1 -1
b3 -1
b7E -1, 2

(S)

information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime.³

(U)

3. ~~(S//NF)~~

[Redacted]

b7E -1, 2

[Redacted]

(U)

4. ~~(S//NF)~~ Ad Hoc Systems -- An ad hoc system is any FBI application, program, device,

or process that does not meet the definition of Electronic and Data Storage System above, that is not governed by Section III.F, and that retains or provides access to raw FISA-acquired information. Ad hoc systems may only be used by FBI personnel who are engaged in or assisting with a particular investigation and when such FBI personnel have reasonably determined that for technical, analytical, operational or security reasons they cannot fully, completely, efficiently or securely review or analyze raw FISA-acquired information in an electronic and data storage system.

[Redacted]

[Redacted]

(U)

~~(S//NF)~~

[Redacted]

b1 -1
b3 -1
b7E -1, 2

[Redacted]

[Redacted]

(S)

C. (U) **Additional Provisions Regarding Access, Review, and Use of FISA-acquired information**

1. (U) Review and use of FISA-acquired information retained in any form.

a. (U) *General.* The FBI may make raw FISA-acquired information available to authorized personnel on a continuing basis for review, translation, analysis, and use in accordance with these procedures. Authorized personnel may continue to access raw FISA-acquired information to determine whether it reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime notwithstanding the fact that other FBI personnel previously may have reviewed such information and determined that it did not reasonably appear to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime at the time of such review.

(U) FBI personnel with authorized access to raw FISA-acquired information may review, translate, copy, transcribe, analyze, summarize, and use all such information only in accordance with these procedures and FISA and only as necessary for the purpose of evaluating or determining whether it reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime. Such personnel shall exercise reasonable judgment in making such evaluations or determinations.

b. (U) *Information meeting criteria.* Once FBI personnel have assessed that raw FISA-acquired information meets one of these criteria, the FBI may retain that information for further investigation and analysis and may disseminate it in accordance with these procedures. Pursuant

to 50 U.S.C. §§ 1801(h)(3) and 1821(4)(C), however, information that is assessed to be evidence of a crime but not to be foreign intelligence information or necessary to understand foreign intelligence information may only be retained and disseminated for law enforcement purposes.

c. (U) *United States person identities.* Before using FISA-acquired information for the purpose of further investigation, analysis, or dissemination, the FBI shall strike, or substitute a characterization for, information of or concerning a United States person, including that person's identity, if it does not reasonably appear to be foreign intelligence information, to be necessary to understand or assess the importance of foreign intelligence information, or to be evidence of a crime. Processing or analyzing FISA-acquired information within an electronic and data storage system or ad hoc system does not trigger this requirement. This requirement is also not triggered by transferring FISA-acquired information between or among electronic and data storage systems, ad hoc systems, collection platforms, or systems used solely for audits and oversight.

b7E -1, 2

d. (U) *Disclosure and dissemination.* The FBI may disclose or disseminate copies, transcriptions, summaries, and other documents containing FISA-acquired information only in accordance with the disclosure and dissemination procedures set forth in Part IV below.

e. (U) *Exculpatory, impeachment, and discoverable material.* The FBI shall retain FISA-acquired information that is not foreign intelligence information that has been reviewed and reasonably appears to be exculpatory or impeachment material for a criminal proceeding, or reasonably appears to be discoverable in a criminal proceeding, and shall treat that information as if it were evidence of a crime.

b1 -1
b3 -1
b7E -1, 2

(U)

~~(S//NF)~~ *Third-Party Information*

[Redacted]

(S)

[Large Redacted Area]

b1 -1
b3 -1
b7E -1, 2

g. (U) *Sensitive Information*. Particular care should be taken when reviewing information that is sensitive information, as defined below. No sensitive information may be used in an analysis or report (such as an Electronic Communication (EC)) unless it is first determined that such information reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information or assess its importance, or evidence of a crime. Information that reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information, or necessary to assess the importance of foreign intelligence information may be retained, processed, and disseminated in accordance with these procedures even if it is sensitive information. Information that reasonably appears to be evidence of a crime may be retained, processed, and disseminated for law enforcement purposes in accordance with these procedures, even if it is sensitive information. Sensitive information consists of:

b3 -1
b7E -1

2. (U) Procedures Regarding Access to FISA-acquired Information Retained in Electronic Form. The FBI may grant access to FISA-acquired information to all authorized personnel in accordance with policies established by the Director, FBI, in consultation with the Attorney General or a designee. The FBI's policies regarding access shall vary according to whether access includes raw FISA-acquired information, and shall be consistent with the FBI's foreign intelligence information-gathering and information-sharing responsibilities, and shall include provisions:

- a. Permitting access to FISA-acquired information only by individuals who require access in order to perform their job duties or assist in a lawful and authorized governmental function;
- b. Requiring the FBI to maintain accurate records of all persons to whom it has granted access to FISA-acquired information; and
- c. Requiring training on these minimization procedures and the FBI's policies regarding access to raw FISA-acquired information before granting access to raw FISA-acquired information.

(U) The FBI shall provide such policies to the Court when these procedures go into effect. Thereafter, the FBI shall provide any new policies or materially modified policies to the Court on a semiannual basis.

D. (U) Electronic and Data Storage Systems

1. (U) **Access to information and auditing requirement.** The FBI shall maintain accurate records of all persons who have accessed FISA-acquired information in electronic and data storage systems and audit its access records regularly to ensure that FISA-acquired information is only accessed by authorized individuals, including FBI personnel and the individuals referenced in Sections III.H.3 and V.A of these procedures.

2. (U) **Marking.** The FBI shall require the primary case agent(s) and his/her/their designees (hereinafter "case coordinator(s)") to control the marking of raw FISA-acquired information in a particular case that is maintained in an electronic and data storage system. A marking, for example, would include an indication that the information is foreign intelligence information. The FBI shall identify FISA-acquired information in electronic and data storage systems that has been reviewed and whether that information has been determined to reasonably appear to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime.

3. (U) Queries.

a. (U) Users who are authorized to have access to raw FISA-acquired information in electronic and data storage systems that contain raw FISA-acquired information may query datasets containing such raw FISA-acquired information in such systems to find, extract, review, translate, and assess whether such information reasonably appears to be foreign intelligence

information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime.

b. (U) To the extent reasonably feasible, authorized users with access to raw FISA-acquired information must design such queries to find and extract foreign intelligence information or evidence of a crime. Authorized users with access to raw FISA-acquired information in an electronic and data storage system may process the results of an appropriate query in accordance with Section III.C above.

(U) c. ~~(S//NF)~~ The FBI shall maintain records of all queries, used by those with access to raw FISA-acquired information to query electronic and data storage systems

b1 -1
b3 -1
b7E -1,2

[Redacted]

(S)

d. (U) For purposes of this section, the term query does not include a user's query of an FBI electronic and data storage system that contains raw FISA-acquired information, where the user does not receive raw FISA-acquired information in response to the query either because the user has not been granted access to the raw FISA-acquired information, or because a user who has been granted such access has limited the query such that it cannot return raw FISA-acquired information.

[Redacted]

b1 -1
b3 -1
b7E -2

(S)

4. (U) **Retention Time Limits.** The FBI is authorized to retain data in electronic and data storage systems as follows:

a. (U) *Standard for Retention.* These Procedures do not limit the retention of information that reasonably appears to be foreign intelligence information, necessary to understand foreign intelligence information or assess its importance, or evidence of a crime.

b. (U) *Information that has not been reviewed.* Raw FISA-acquired information that has been retained but never reviewed shall be destroyed five years from the expiration date of the docket authorizing the collection unless specific authority is obtained from an executive at FBI Headquarters in a position no lower than Assistant Director (AD) and from NSD to retain the material, and the FISC approves a new retention period upon a finding that such modification is consistent with the applicable statutory definition of "minimization procedures."

(U) ~~(S//NF)~~ *Information that has been reviewed but not identified as meeting the applicable standard.* FISA-acquired information that has been retained and reviewed, but not identified as information that reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime, may be retained and be fully accessible to authorized personnel for further review and analysis for [redacted] from the expiration date of the docket authorizing the collection.

b1 -1
b3 -1

(S) i. [redacted] from the expiration date of the docket authorizing the collection, access to such information contained in electronic and data storage systems shall be limited to search capabilities that would produce notice to an authorized user that information responsive to a query exists. Approval from an executive at FBI Headquarters in a position no lower than AD, or such person's designee, is required to gain full access to this information.

ii. FISA-acquired information that has been retained and reviewed, but not identified as information that reasonably appears to be foreign intelligence, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime, shall be destroyed from the expiration date of the docket authorizing the collection unless specific authority is obtained from an executive at FBI Headquarters in a position no lower than AD and from NSD to retain the material, and the FISC approves a new retention period upon a finding that such modification is consistent with the applicable statutory definition of "minimization procedures."

b1 -1
b3 -1

(U) 5. ~~(S//NF)~~ **Retention of Attorney-Client Communications.** This section governs the retention of attorney-client communications in electronic and data storage systems. The subparagraphs relating to attorney-client privileged communications apply regardless of whether such communications are of or concerning U.S. persons. In certain cases, however, the Government may propose and/or the FISC may order the use of supplemental procedures. FBI personnel shall consult as appropriate with FBI Division Counsel, the FBI Office of General Counsel, or the NSD to determine whether a communication is privileged.

(U) a. ~~(S//NF)~~ *Target charged with a crime pursuant to the United States Code.* As soon as the FBI knows that a target is charged with a crime pursuant to the United States Code, the FBI shall implement procedures that ensure that the target's attorney-client privilege is protected.

These procedures shall include the following, unless otherwise authorized by the FISC:

i. Establishment of a review team of one or more monitors and/or reviewers, who have no role in the prosecution of the charged criminal matter, to initially access and review information or communications acquired from a surveillance or search of a target who is charged with a crime pursuant to the United States Code;



(S)

b1 -1
b3 -1
b7E -1,2

[Redacted]

(S)

b1 -1
b3 -1
b7E -1,2

[Redacted]

(S)

b1 -1
b3 -1
b7E -1,2

[Redacted]

[Redacted]

(S)

b1 -1
b3 -1
b7E -1,2

vi. As soon as FBI personnel recognize that communications between the person under criminal charges and his attorney have been acquired [Redacted]

[Redacted]

the FBI shall ensure that whenever any user reviews information or

(S)

b1 -1
b3 -1

communications acquired [Redacted] in an FBI electronic and data storage system containing raw FISA-acquired information, he receives electronic

(S)

notification that attorney-client communications have been acquired [Redacted]

(S)

(S) [redacted] The purpose of the notification is to alert others who may review this information that they may encounter privileged communications.⁶

b1 -1
b3 -1

(U) ~~(S//NF)~~ Target charged with a non-Federal crime in the United States and persons other than a target charged with a crime in the United States. FBI monitors and other personnel with access to FISA-acquired information shall be alert for communications that may be (i) between a target who is charged with a non-Federal crime in the United States and the attorney representing the individual in the criminal matter, or (ii) between a person other than a target charged with a crime in the United States and the attorney representing the individual in the criminal matter.

(U) ~~(S//NF)~~ As soon as FBI personnel know that a target is charged with a non-Federal crime in the United States or someone other than the target who appears to regularly use the targeted facility, place, premises or property is charged with a crime in the United States, they shall notify the Chief Division Counsel, FBI Office of General Counsel, and NSD to determine whether supplemental procedures or a separate monitoring team are required. In the absence of such supplemental procedures or a separate monitoring team, as soon as FBI personnel recognize that they have acquired a communication between (i) a target who is charged with a non-Federal crime in the United States and the attorney representing the individual in the criminal matter, or (ii) a person other than a target charged with a crime in the United States and the attorney

[redacted]

(S)
b1 -1
b3 -1
b7E -1,2

b1 -1
b3 -1
b7E -1,2

representing the individual in the criminal matter, the FBI shall implement procedures that include the following:

(S) [Redacted]

[Redacted] the FBI shall seal the original record or portion thereof containing that privileged communication, label it as containing privileged communications, forward the original recording containing the privileged communication to the NSD for sequestration with the FISC, and destroy all other copies of the privileged communication that are accessible in hard copy or electronically to anyone other than system administrators or similar technical personnel.

b1 -1
b3 -1
b7E -1,2

(S) [Redacted]

v. As soon as FBI personnel recognize that communications between the person under criminal charges and his attorney have been acquired [Redacted]

(S) [Redacted] the FBI shall ensure that whenever any user reviews information or communications acquired [Redacted] which are in an FBI electronic and data storage system containing raw FISA-acquired information, he receives electronic notification that attorney-client communications have been acquired during the

(S)
b1 -1
b3 -1
b7E -1, 2

(S) [Redacted]

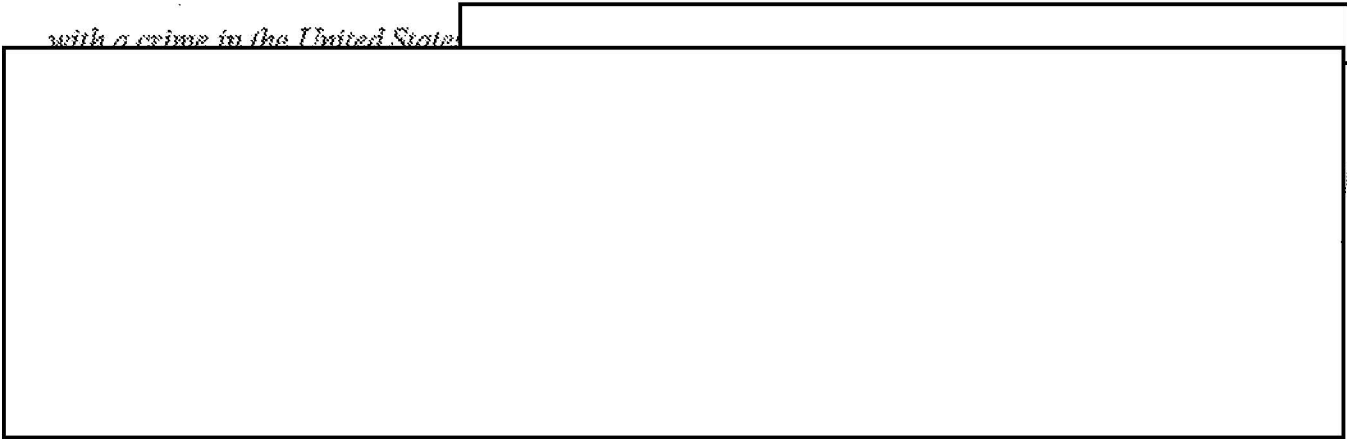
(S)
b1 -1
b3 -1
b7E -1,2

search or surveillance. The purpose of the notification is to alert others who may review this information that they may encounter privileged communications.⁸

(U)

c. ~~(S//NF)~~ *Privileged communications involving targets and other persons not charged*

with a crime in the United States



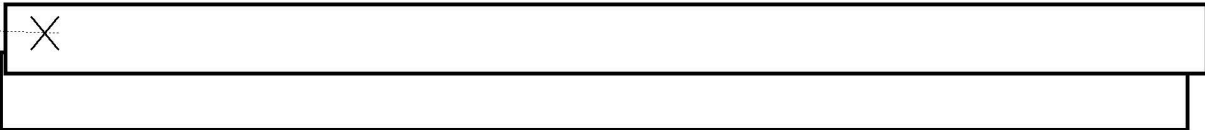
(S)

b1 -1
b3 -1
b7E -1, 2

(U)

~~(S//NF)~~ FISA-acquired communications of a target or other person not charged with a crime in the United States that are attorney-client privileged and retained by FBI in any form shall not be disseminated to any other agency within the Intelligence Community without the approval of the FBI Office of the General Counsel or FBI Division Counsel. Before any such dissemination, the Office of the General Counsel or FBI Division Counsel and FBI personnel shall make reasonable efforts to (1) use other non-privileged sources, including communications previously reviewed by the FBI personnel, for any information in the privileged communication, if available, and (2) tailor the dissemination to minimize or eliminate the disclosure of an attorney-client privileged communication, consistent with the need to disseminate foreign intelligence information or evidence of a crime.

(U)



b7E -1, 2

(U) ~~(S//NF)~~ Before disseminating any attorney-client privileged communication that otherwise meets the standards for dissemination outside the United States Intelligence Community, the FBI must obtain the approval of the Attorney General or the Assistant Attorney General for National Security

b1 -1
b3 -1
b7E -1, 2

[Redacted]

(S)

(U) ~~(S//NF)~~ All disseminations of privileged communications shall include language advising recipients that (1) the report contains information that is subject to the attorney-client privilege, (2) the information is provided solely for intelligence or lead purposes, and (3) the information may not be disseminated further or used in any trial, hearing, or other proceeding without express approval by the FBI. The FBI may only grant such approval if authorized by the Attorney General or the Assistant Attorney General for National Security.

[Redacted]

(S)

b1 -1
b3 -1
b7E -1, 2

E. (U) **Ad Hoc Systems.** The following provisions apply to FISA-acquired information in ad hoc systems in addition to those discussed in Section III.C above.

1. (U) **Standard for Use.**

(U) ~~(S//NF)~~ If FBI personnel who are engaged in or assisting with a particular investigation reasonably determine that for technical, analytical, operational or security reasons they cannot fully, completely, efficiently or securely review or analyze raw FISA-acquired information in an electronic and data storage system, the FBI may utilize ad hoc systems to review or analyze such information.

2. (U) **Disclosure, Dissemination, Compliance, and Privilege.** The dissemination and disclosure of FISA-acquired information from ad hoc systems are subject to the Dissemination and Disclosure provisions in Section IV. Ad hoc systems are subject to the Compliance provisions in Section V. The provisions in subparagraph 6 below relating to attorney-client privileged communications apply regardless of whether such communications are of or concerning U.S. persons.

3. (U) **Access to and Identification of FISA-Acquired Information.**

a. (U) Access to raw FISA-acquired information contained in an ad hoc system shall be limited to individuals engaged in or assisting with the particular investigation, individuals conducting or aiding in the assessment or analysis of that information in support of that investigation, and system administrators or other similar technical personnel who require this access in order to perform their official duties.

b. (U) The FBI shall notify personnel with access to the ad hoc system that it includes raw FISA-acquired information.

4. (U) Retention of FISA-Acquired Information.

a. (U) Raw FISA-acquired information concerning unconsenting U.S. persons may be retained in an ad hoc system in order to determine whether the information reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime.

b. (U) Any FISA-acquired U.S. Person information that reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime may be retained in an ad hoc system without time limitation.

(U) c. ~~(S//NF)~~ FISA-acquired U.S. Person information in an ad hoc system that has not been determined to be foreign intelligence information, necessary to understand foreign intelligence information or assess its importance, or evidence of a crime, shall be removed from any ad hoc system no later than five years from the expiration of the docket authorizing the collection of that information,⁹ unless specific authority is

(U) ~~(S//NF)~~ [Redacted] (S)
[Redacted] b1 -1
[Redacted] b3 -1
[Redacted] b7E -1, 2
[Redacted] (S)

obtained from an executive at FBI Headquarters in a position no lower than Assistant Director and NSD to retain the information, and the FISC approves a new retention period upon a finding that such modification is consistent with the applicable statutory definition of "minimization procedures."

(U)

- d. ~~(S//NF)~~ The FBI will keep adequate records to (i) identify persons who either have accessed, or have been granted access to, raw FISA-acquired information in an ad hoc system, (ii) document FISA-acquired information in an ad hoc system that has been determined to be foreign intelligence information, necessary to understand foreign intelligence information or assess its importance, or evidence of a crime, and (3) document the removal of FISA-acquired information as required in Section III.E.4.

5. (U) Analysis and Queries of Raw FISA-Acquired Information.

(U) Users who are authorized to have access to raw FISA-acquired information in an ad hoc system may analyze the data to find, extract, review, translate, and assess whether such information reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime. If datasets which contain raw FISA-acquired information in an ad hoc system are queried, such queries must be designed to find and extract foreign intelligence information or evidence of a crime.

b1 -1
b3 -1
b7E -1, 2

(S)

(U) ~~(S//NF)~~ The FBI shall document such queries to the extent reasonably practicable based on the type of ad hoc system being used. However, the FBI shall not be required to maintain

(S) records [redacted] used to scan raw FISA-acquired information to identify malware. The FBI shall also not be required to maintain records of a system user's actions to sort a defined dataset based upon attributes of the data. [redacted]

b1 -1
b3 -1
b7E -1, 2

(S)

[Large redacted block]

(U) 6. ~~(S//NF)~~ Procedures for Retention of Attorney-Client Communications.

(U) a. ~~(S//NF)~~ Target charged with a crime pursuant to the United States Code, target charged with a non-Federal crime in the United States, and persons other than a target charged with a crime in the United States. As soon as the FBI knows that a target is charged with a crime pursuant to the United States Code, the FBI shall follow the procedures described in Section III.D.5.a. If FBI personnel discover attorney-client privileged communications in an ad hoc system that fall within Section III.D.5.a or b, all such attorney-client privileged communications must immediately be removed from the ad hoc system.

[Redacted block]

(S)
b1 -1
b3 -1
b7E -1, 2

(S)

[Redacted]

b1 -1
b3 -1
b7E -1,2

(U)

b. ~~(S/NF)~~ Other attorney-client privileged communications

[Redacted]

b1 -1
b3 -1
b7E -1,2

(S)

[Redacted]

i. To the extent that the attorney-client privileged communications are accessible in any electronic and data storage system the FBI shall ensure it follows the provisions in

[Redacted]

(S)

b1 -1
b3 -1
b7E -1, 2

[Redacted]

(S)
b1 -1
b3 -1
b7E -1, 2

(S)

[Redacted]

(S)

c. (U) FBI personnel shall consult as appropriate with FBI Division Counsel, the FBI Office of the General Counsel, or NSD to determine whether a communication is privileged.

(U)

F.

~~SECRET//NOFORN~~

(S)

[Redacted]

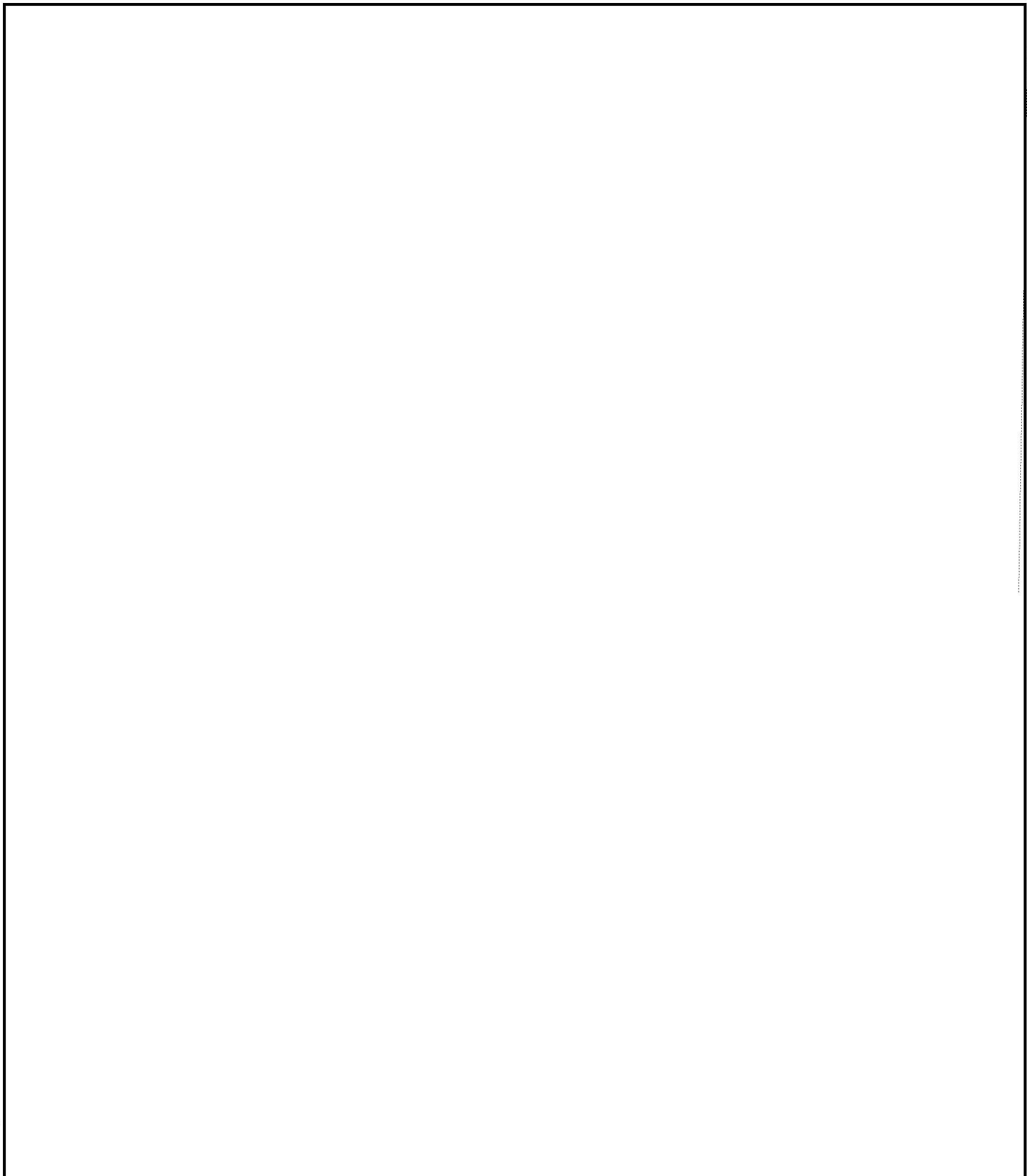
[Redacted]

b1 -1
b3 -1
b7E -1,2

~~SECRET//NOFORN~~

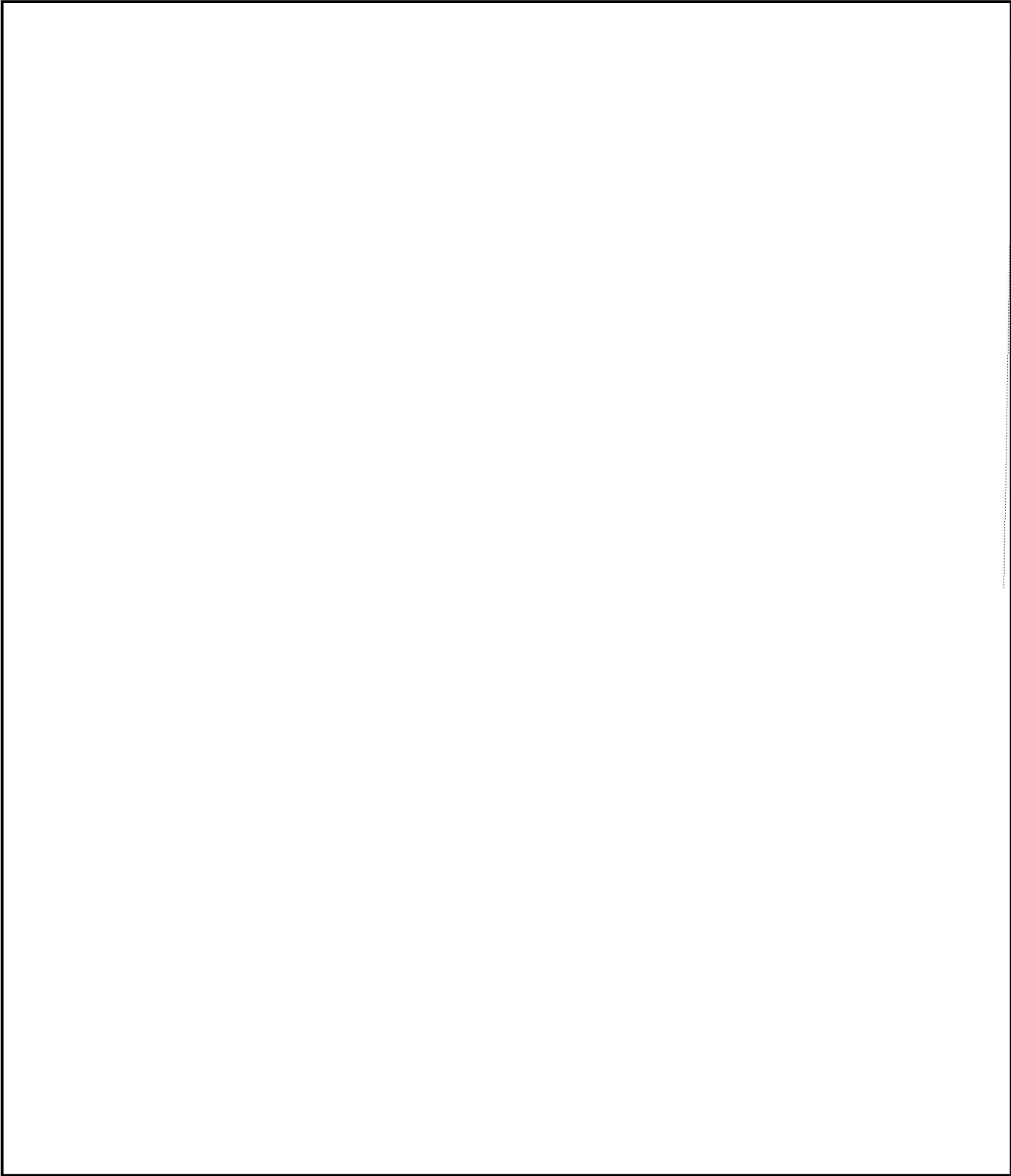
b1 -1
b3 -1
b7E -1,2

(S)



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

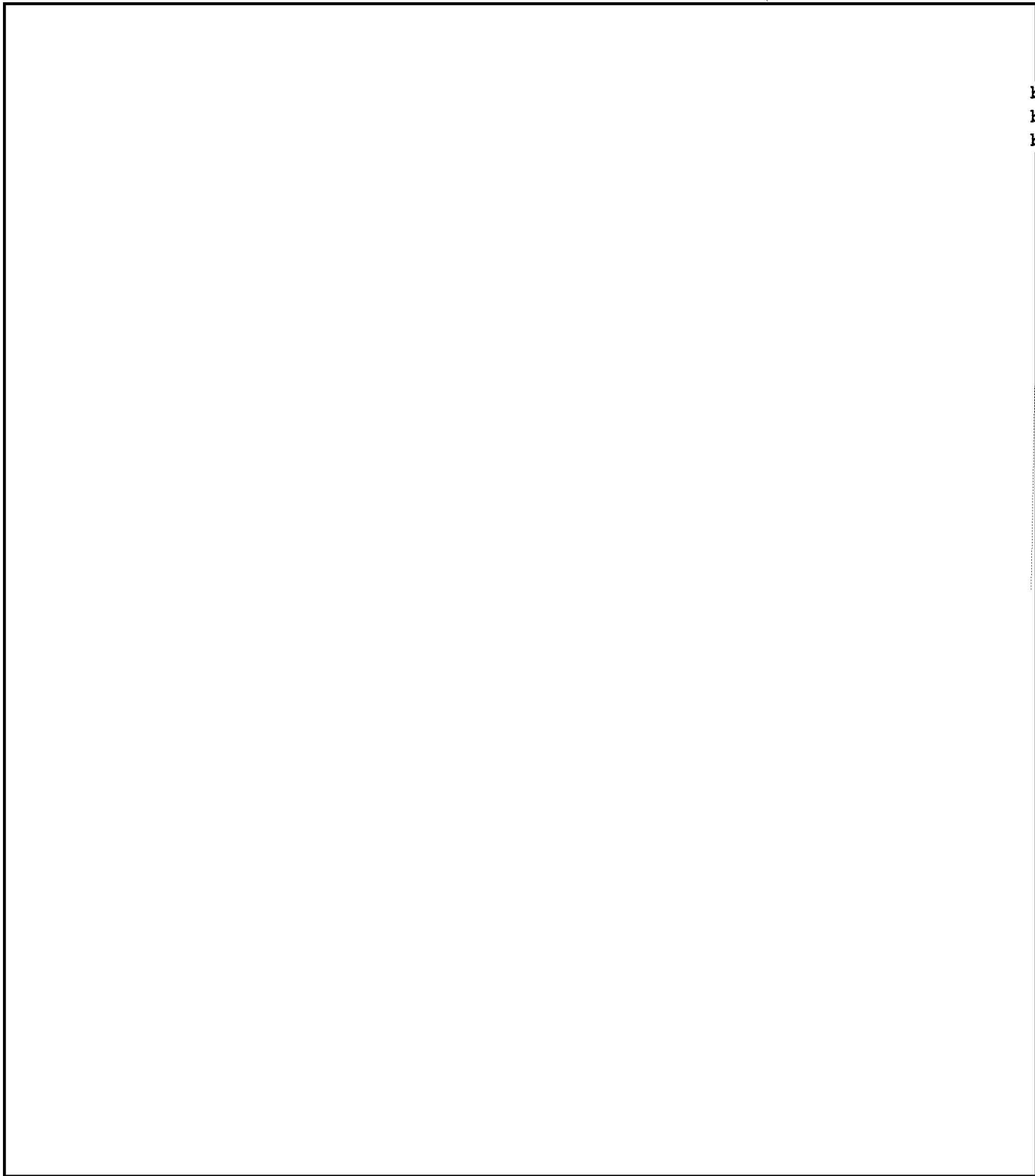


(S)

b1 -1
b3 -1
b7E -1,2

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



(S)

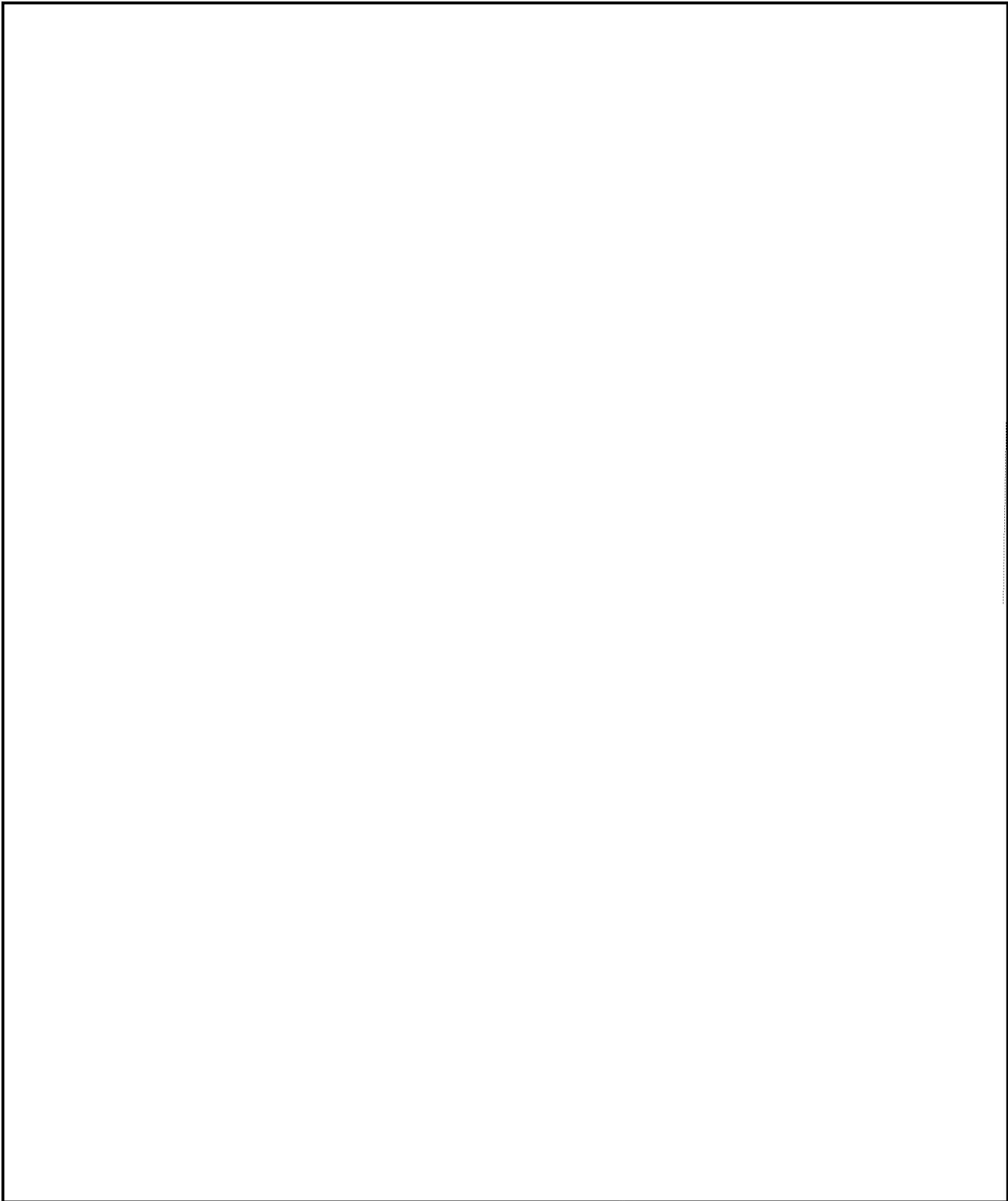
b1 -1

b3 -1

b7E -1,2

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



(S)

b1 -1
b3 -1
b7E -1,2

~~SECRET//NOFORN~~



(S)

b1 -1
b3 -1
b7E -1, 2

II. (U) Additional Procedures for Retention, Use, and Disclosure.

1. **(U) Law Enforcement.** Pursuant to 50 U.S.C. §§ 1806(b) and 1825(c), no information acquired pursuant to an order authorizing electronic surveillance or physical search under FISA shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General. When Attorney General authorization is acquired, FISA-acquired information, including raw FISA-acquired information, may be disclosed for law enforcement purposes in criminal proceedings.

2. **(U) Identities.** The FBI shall ensure that identities of any persons, including United States persons, that reasonably appear to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime, are accessible when a query is conducted or made of FISA-acquired information.

3. **(U) Prosecutors.**

a. **(U)** The FBI may disclose FISA-acquired information, including raw FISA-acquired information, and information derived therefrom, to federal prosecutors and others working at their direction, for all lawful foreign intelligence and law enforcement purposes, including in order to enable the prosecutors to determine whether the information: (1) is evidence

of a crime, (2) contains exculpatory or impeachment information; or (3) is otherwise discoverable under the Constitution or applicable federal law. When federal prosecutors and others working at their direction are provided access to raw FISA-acquired information, they shall be trained on and comply with these and all other applicable minimization procedures.

b. (U) In accordance with applicable Attorney General-approved policies and procedures, federal prosecutors may also disclose FISA-acquired information, when necessary for the prosecutors to carry out their responsibilities, including to witnesses, targets or subjects of an investigation, or their respective counsel, when the FISA-acquired information could be foreign intelligence information or is evidence of a crime. This provision does not restrict a federal prosecutor's ability, in a criminal proceeding, to disclose FISA-acquired information that contains exculpatory or impeachment information or is otherwise discoverable under the Constitution or applicable federal law.

(U) c. ~~(S//NF)~~ The FBI may not provide federal prosecutors and others working at their direction with access to raw FISA-acquired information unless such access is: (a) for foreign intelligence or law enforcement purposes; (b) consistent with their responsibilities as federal prosecutors; and (c) pursuant to procedures established by the Attorney General and provided to the FISC. The procedures established by the Attorney General and provided to the FISC shall include the following:

- i. Access to raw FISA-acquired information must be limited to that which is consistent with their responsibilities as federal prosecutors

and necessary to carry out their responsibilities efficiently during a specific investigation or prosecution;

- ii. Access to raw FISA-acquired information in an FBI electronic and data storage system or ad hoc system must be requested from and approved by an executive at FBI Headquarters in a position no lower than Deputy Assistant Director (DAD) and in coordination with the Deputy General Counsel of the FBI National Security Law Branch or a Senior Executive Service attorney in the National Security Law Branch, and will be considered on a case-by-case basis. Access to raw FISA-acquired information in a form other than in an FBI electronic and data storage system or ad hoc system must be requested from and approved by an executive at FBI Headquarters in a position no lower than Section Chief in the FBI National Security Branch and in coordination with a Section Chief in the FBI National Security Law Branch, and will be considered on a case-by-case basis;
- iii. A request for access must specify to which FBI electronic and data storage system or ad hoc system, FISC docket numbers, and targeted facilities the prosecutor needs access, why such access is necessary, and the duration of such access;

- iv. All individuals receiving authorization to have access to raw FISA-acquired information in an FBI electronic and data storage system or ad hoc system must receive user training on the system(s) to which they seek access, and training on the standard minimization procedures and any relevant supplemental minimization procedures applicable to the information to which they have access;
- v. Access shall be terminated no later than the conclusion of the relevant investigation or prosecution; and
- vi. Federal prosecutors may immediately be given access to raw FISA-acquired information if FBI personnel determine that an immediate threat to life or of serious damage to property necessitates immediate access, and if such immediate access is given to federal prosecutors, notification shall be made to FBI Headquarters, FBI's Office of General Counsel, and NSD.

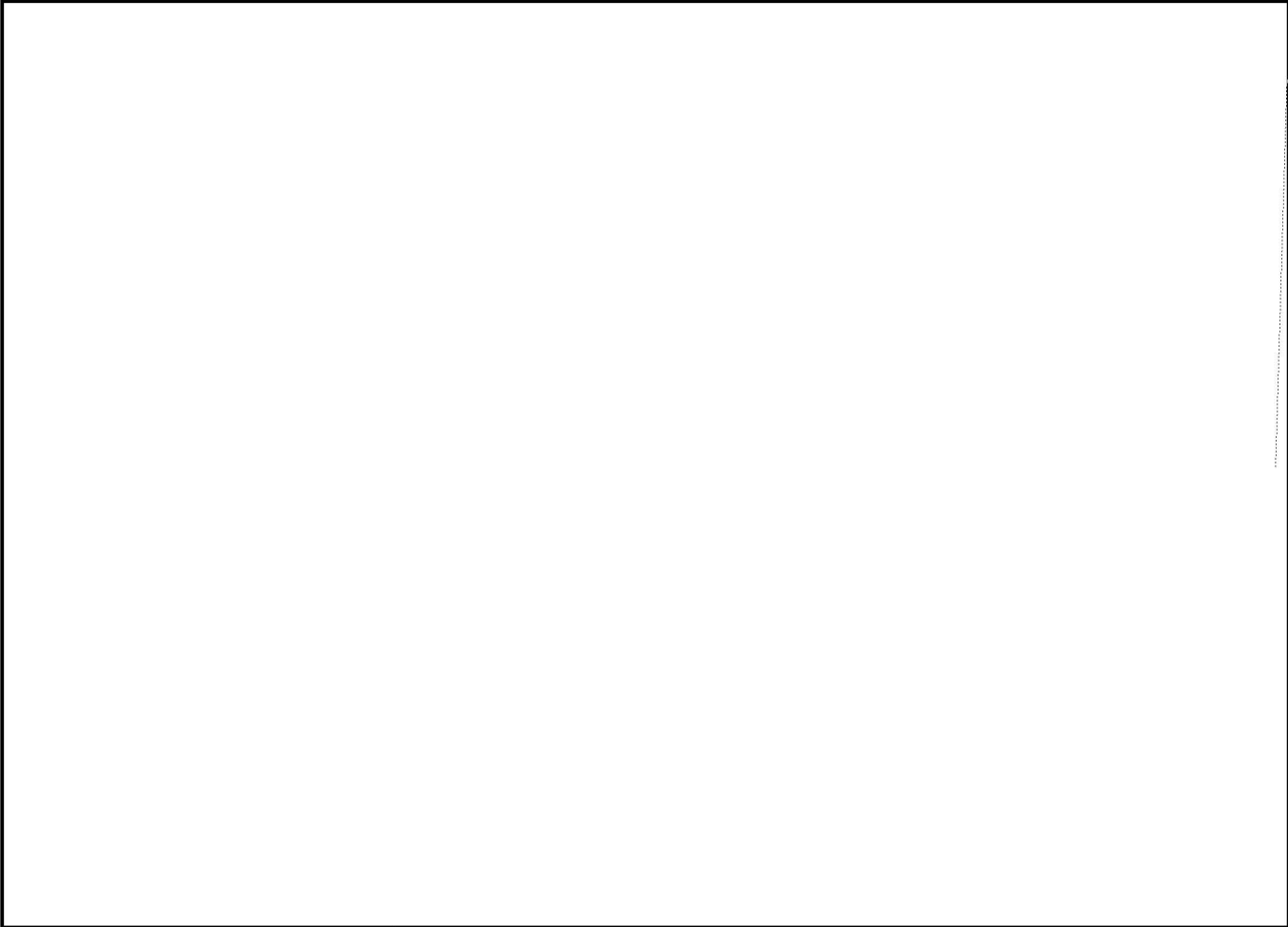
I. (U) Other Time Limits for Retention. In general, the FBI may retain FISA-acquired information that reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime.

1.

[Redacted]

(S)

b1 -1
b3 -1
b7E -1,2



(S)

b1 -1
b3 -1
b7E -1,2

(U) 3. ~~(S//NF)~~ Backup and evidence copies in FBI systems. The FBI may retain on a system emergency backup or original evidence copies of information provided that only system administrators or other similar technical personnel have access to such information to perform their official duties. No intelligence analysis may be performed in such systems, nor may the data be accessed within such systems for the purpose of performing intelligence analysis. In the event that such information must be used to restore lost, destroyed, or inaccessible data, or to provide an original evidence copy, the FBI shall apply these procedures, including any applicable retention time limits, to the transferred data.

b1 -1
b3 -1
b7E -1,2

(S)



[Redacted]

(S)

b1 -1
b3 -1
b7E -1,2

4. (U) **Information retained in connection with litigation matters.** The FBI may temporarily retain specific FISA-acquired information that would otherwise have to be destroyed pursuant to these minimization procedures:

[Redacted]

[Redacted]

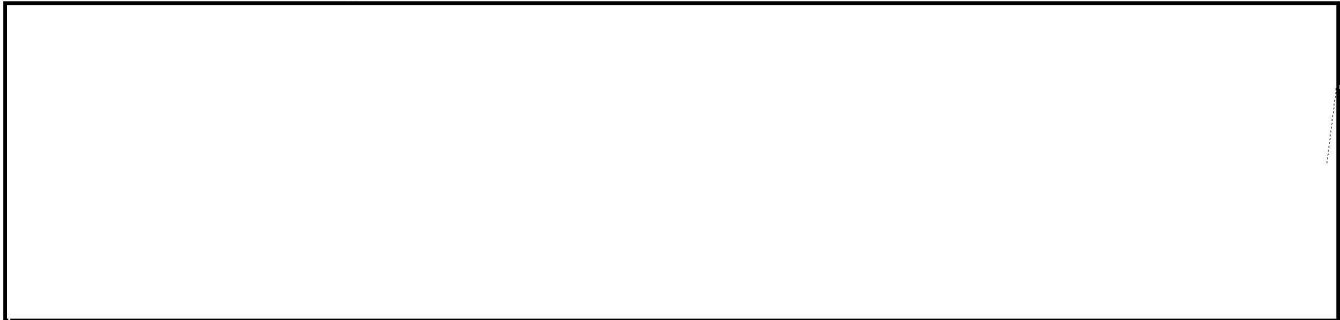
(S)

(S)

b1 -1
b3 -1
b7E -1,2

(U) 5. ~~(S//NF)~~ **Encrypted information.** Raw FISA-acquired information that reasonably appears to be encrypted or to contain secret meaning may be maintained for any period of time during which such material is subject to, or of use in, cryptanalysis or otherwise deciphering secret meaning. Access to such information shall be restricted to those FBI personnel engaged in cryptanalysis or deciphering secret meaning. Nonpublicly available information concerning unconsenting U.S. persons retained under this subsection may only be

used for cryptanalysis, and not for any other purpose, unless the FBI determines that it may also be retained under a separate provision of these Procedures.



(S)

b1 -1
b3 -1
b7E -1,2

(U) 6. ~~(S//NF)~~ **Retention in other form.** FISA-acquired information retained by the FBI in any other form shall be destroyed in accordance with the Attorney General Guidelines and relevant National Archives and Records Administration procedures regarding the retention of information in FBI investigations.

IV. (U) DISSEMINATION AND DISCLOSURE

A. (U) **Dissemination of Foreign Intelligence Information to Federal, State, Local and Tribal Officials and Agencies.**

(U) The FBI may disseminate FISA-acquired information that reasonably appears to be foreign intelligence information or is necessary to understand foreign intelligence information or assess its importance in accordance with Sections IV.A.1 and IV.A.2 to federal, state, local and tribal officials and agencies with responsibilities relating to national security that require access to foreign intelligence information. Such information may be disseminated only consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

1. (U) Foreign Intelligence Information as defined in 50 U.S.C. § 1801(e)(1).

(U) The FBI may disseminate to federal, state, local and tribal officials and agencies FISA-acquired information concerning United States persons that reasonably appears to be necessary to the ability of the United States to protect against: (i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (ii) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or (iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

2. (U) Foreign Intelligence Information as defined in 50 U.S.C. § 1801(e)(2).

(U) The FBI may disseminate to federal, state, local and tribal officials and agencies FISA-acquired information concerning United States persons that reasonably appears to be necessary: (i) to the national defense or the security of the United States; or (ii) the conduct of the foreign affairs of the United States. Such information shall not be disseminated, however, in a manner that identifies a United States person, unless such person's identity is necessary to understand foreign intelligence information or to assess its importance.

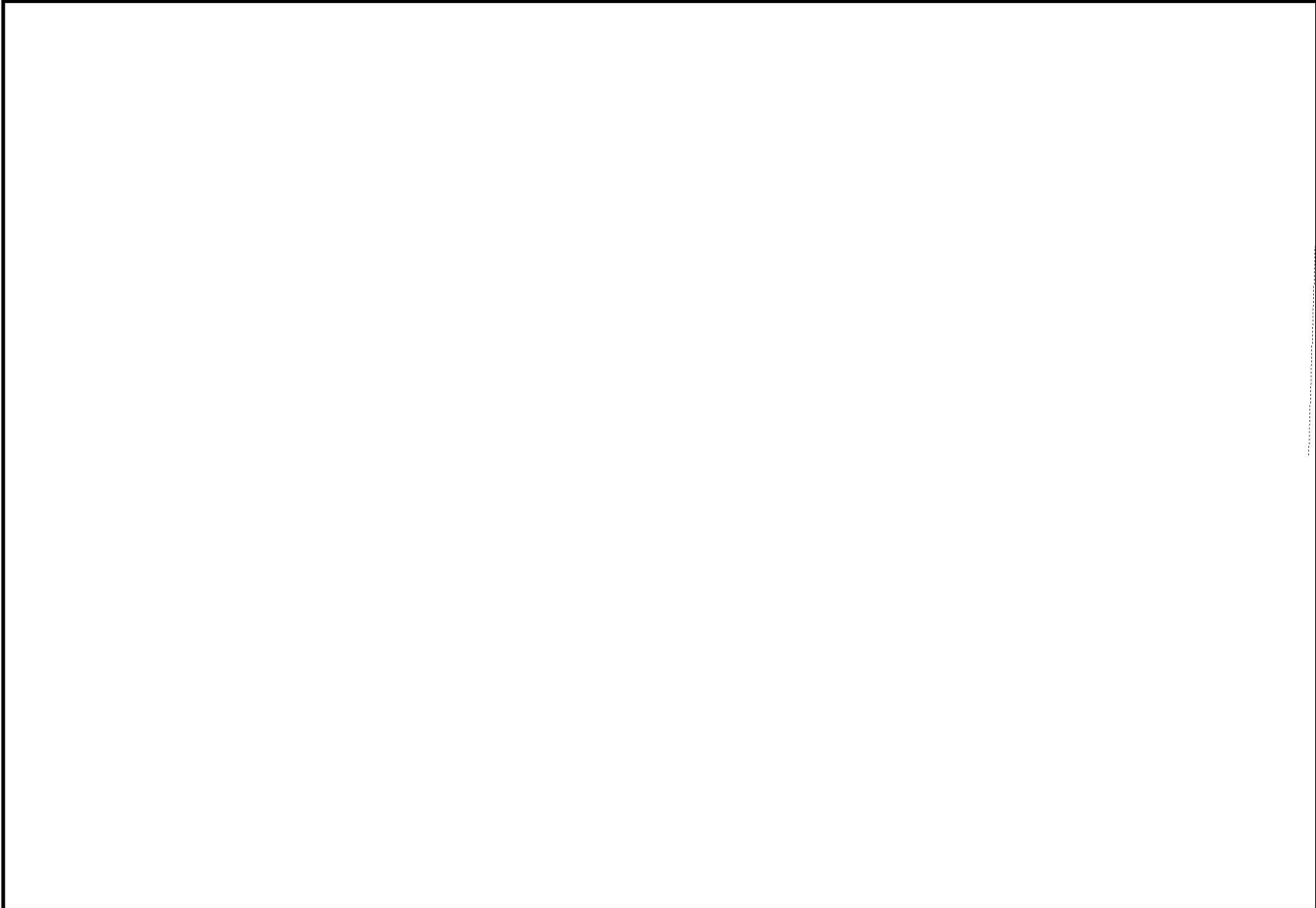
B. (U) Dissemination of Evidence of a Crime to Federal, State, Local and Tribal Officials, and the National Center for Missing and Exploited Children.

(U) The FBI may disseminate, for a law enforcement purpose, FISA-acquired information concerning a United States person that reasonably appears to be evidence of a crime but not foreign intelligence information to federal, state, local, and tribal law enforcement officials and agencies. The FBI may also disseminate, for law enforcement purposes, FISA-acquired information that reasonably appears to be evidence of a crime related to child

exploitation material, including child pornography, to the National Center for Missing and Exploited Children (NCMEC). The FBI shall disseminate such FISA-acquired information in a manner consistent with the requirements of Section III.G.

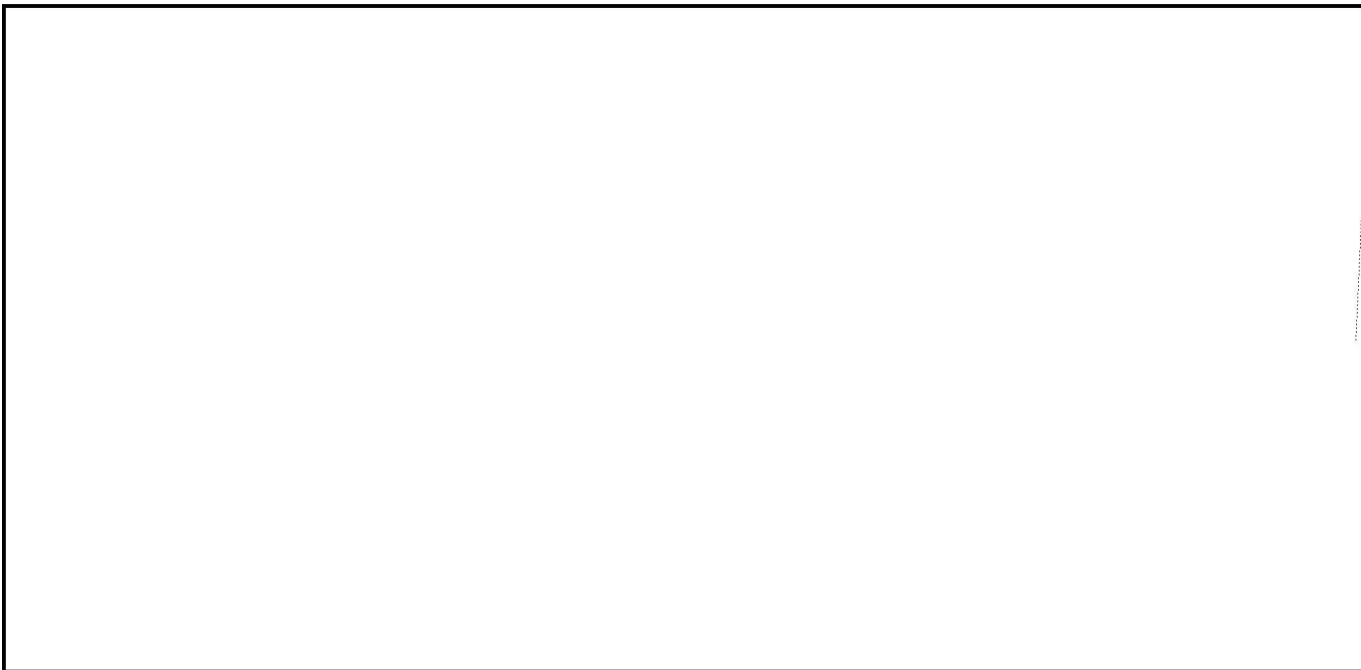
C. (U) Dissemination to Foreign Governments.

~~(S//NF)~~ The FBI may disseminate FISA-acquired information concerning United States persons, which reasonably appears to be foreign intelligence information, is necessary to understand foreign intelligence information or assess its importance, or is evidence of a crime being disseminated for a law enforcement purpose, to officials of foreign governments, as follows:




(S)

b1 -1
b3 -1
b7E -1,2



(S)

b1 -1
b3 -1
b7E -1,2

3. (U) The Attorney General, in consultation with the DNI or a designee, may authorize 

b3 -1
b7E -1

 Prior to

granting such authorization, those officials shall consider, among other things: (1) whether such use is consistent with the national security interests of the United States, and (2) the effect of such use on any identifiable United States person.

4. (U) The FBI shall make a written record of each dissemination approved pursuant to this section, and information regarding such disseminations and approvals shall be

b3 -1
b7E -1



D. (U) Disclosure of Raw FISA-acquired Information for Technical or Linguistic Assistance.

(U) ~~(S//NF)~~ The FBI may obtain information or communications that, because of their technical or linguistic content, may require further analysis by other federal agencies (collectively, "assisting federal agencies") to assist the FBI in determining their meaning or significance. Consistent with the other provisions of these procedures, the FBI is authorized to disclose FISA-acquired information [redacted]

b1 -1
b3 -1
b7E -1,2

[redacted] to assisting federal agencies for further processing and analysis. The FBI may also disclose, for the purpose of obtaining technical or linguistic assistance, FISA-acquired information that reasonably appears to be evidence of a crime related to child exploitation material, including child pornography.

b1 -1
b3 -1
b7E -1,2

[redacted] (S)

[redacted] to the National Center for Missing and Exploited Children (NCMEC) for further processing and analysis. The following restrictions apply with respect to any materials so disclosed:¹⁴

- 1. (U) Disclosure to assisting federal agencies and NCMEC will be solely for translation or analysis of such information or communications. Assisting federal agencies and NCMEC will make no use of any information or any communication of or concerning any person except to provide technical or linguistic assistance to the FBI.

¹⁴ (U) The FBI will advise NCMEC of the need to comply with the restrictions described in Section IV.D with respect to information disclosed to NCMEC pursuant to this section.

2. (U) Disclosure will be only to those personnel within assisting federal agencies or NCMEC involved in the translation or analysis of such information or communications. The number of such personnel shall be restricted to the extent reasonably feasible. There shall be no further disclosure of this raw data within assisting federal agencies or NCMEC.

(U) 3. ~~(S//NF)~~ Assisting federal agencies and NCMEC shall make no permanent agency record of information or communications of or concerning any person referred to in FISA-acquired information [redacted]

b1 -1
b3 -1
b7E -1,2

[redacted]

(S)

disclosed by the FBI to assisting federal agencies or NCMEC, provided that assisting federal agencies or NCMEC may maintain such temporary records as are necessary to enable them to assist the FBI with the translation or analysis of such information. Records maintained by assisting federal agencies or NCMEC for this purpose may not be disclosed within the assisting federal agency or NCMEC, except to personnel involved in providing technical assistance to the FBI.

(U) 4. ~~(S//NF)~~ Upon the conclusion of such technical assistance to the FBI, the FISA-acquired information [redacted]

[redacted]

(S) b1 -1
b3 -1
b7E -1,2

disclosed to assisting federal agencies and NCMEC, will either be returned to the FBI or be destroyed, with an accounting of such destruction made to the FBI.

5. (U) Any information that assisting federal agencies or NCMEC provide to the FBI as a result of such technical assistance may be disseminated by the FBI in accordance with the applicable minimization procedures.

(U) E. ~~(S//NF)~~ [redacted] (S)

b1 -1
b3 -1
b7E -1, 2

(U) ~~(S//NF)~~ The FBI may disclose to the Central Intelligence Agency (CIA) and National Security Agency (NSA) raw FISA-acquired information that relates to [redacted] (S)

~~(U)~~ (U) [redacted]

b7E -1, 2

(U) 1. ~~(S//NF)~~ [redacted]

[redacted]

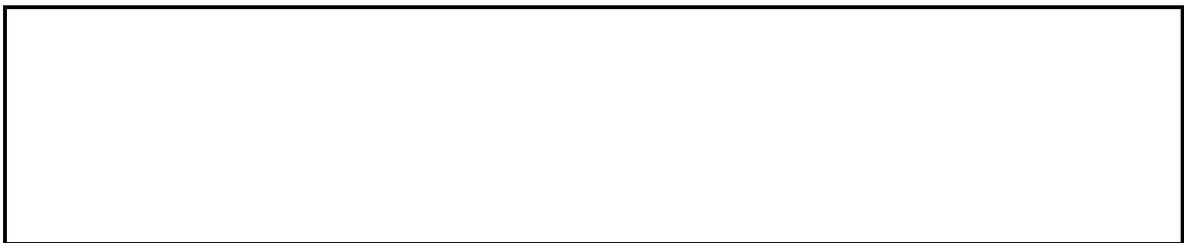
(U) 2. ~~(S//NF)~~ Nothing in this Section shall prohibit or otherwise limit FBI's authority under other provisions of these procedures to disseminate to CIA or NSA information acquired pursuant to the Act and to which governing minimization procedures have been applied.

F. (U) **Dissemination of Foreign Intelligence Information for Terrorist Screening.**

(U) ~~(S//NF)~~ In addition to dissemination authorized under other provisions herein, foreign intelligence information, as defined in Section 1801(e), may be disseminated to federal, state, local, territorial, and tribal authorities, foreign officials and entities, and private sector entities that have a substantial bearing on homeland security for the purposes of and in accordance with Homeland Security Presidential Directive 6 and the Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism and the addenda thereto.

(U) G. ~~(S//NF)~~ **Disclosure to the National Counterterrorism Center (NCTC) of Information Acquired in Cases Related to Terrorism or Counterterrorism.**

(U) I. ~~(S//NF)~~ In addition to other disclosures permitted in these procedures, the FBI may provide to NCTC:



b7E -1, 2

b. information in FBI general indices, including the Automated Case Support (ACS) system and any successor system, provided that such access is limited to case classifications that are likely to contain information related to terrorism or counterterrorism.

NCTC's receipt of information described in (a) and (b) above is contingent upon NCTC's application of NCTC minimization procedures approved by the FISC with respect to such information.

(U) 2. ~~(S//NF)~~ Nothing in this Section shall prohibit or otherwise limit FBI's authority under other provisions of these procedures to disseminate to NCTC information acquired pursuant to the Act and to which governing minimization procedures have been applied.

(U) 3. ~~(S//NF)~~ b7E -1, 2

(U) 4. ~~(S//NF)~~ For every surveillance or search from which FBI discloses raw

 b7E -1, 2

(U) **H. (U) Dissemination of Foreign Intelligence Information or Evidence of a Crime Involving Computer Intrusions or Attacks to Private Entities and Individuals.**

~~(S//NF)~~ The FBI may disseminate FISA-acquired information that reasonably appears to be foreign intelligence information, is necessary to understand foreign intelligence information or assess its importance, or is evidence of a crime and that it reasonably believes may assist in

the mitigation or prevention of computer intrusions or attacks to private entities or individuals that have been or are at risk of being victimized by such intrusions or attacks, or to private entities or individuals (such as Internet security companies and Internet Service Providers) capable of providing assistance in mitigating or preventing such intrusions or attacks. Wherever reasonably practicable, such dissemination should not include United States person identifying information unless the FBI reasonably believes it is necessary to enable the recipient to assist in the mitigation or prevention of computer intrusions or attacks.

I. (U) Dissemination to Private Entities and Individuals of Foreign Intelligence Information or Evidence of a Crime Involving a Matter of Serious Harm.

(U) ~~(S//NF)~~ The FBI may disseminate FISA-acquired information that reasonably appears to be foreign intelligence information, is necessary to understand foreign intelligence information or assess its importance, or is evidence of a crime to a private individual or entity in situations where the FBI determines that said private individual or entity is capable of providing assistance in mitigating or preventing serious economic harm or serious physical harm to life or property. Wherever reasonably practicable, such dissemination should not include United States person identifying information unless the FBI reasonably believes it is necessary to enable the recipient to assist in the mitigation or prevention of the harm. The FBI will report to NSD all disseminations made pursuant to this paragraph within ten business days of such dissemination. NSD will promptly report to the FISC any disseminations made pursuant to this paragraph.

V. (U) COMPLIANCE

A. (U) Oversight.

(U) To ensure compliance with these procedures, the Attorney General, through the Assistant Attorney General for National Security or other designee, shall implement policies and procedures that ensure the good faith compliance with all of the requirements set forth herein, and shall conduct periodic minimization reviews, including reviews at FBI Headquarters, field offices, and U.S. Attorney's Offices that receive raw FISA-acquired information pursuant to Section III of these procedures. The Attorney General and the NSD or other designee of the Attorney General shall have access to all FISA-acquired information to facilitate minimization reviews and for all other lawful purposes.

(U) To assess compliance with these procedures, minimization reviews shall consist of reviews of documents, communications, audit trails, or other information. They shall include, as appropriate, but are not limited to:

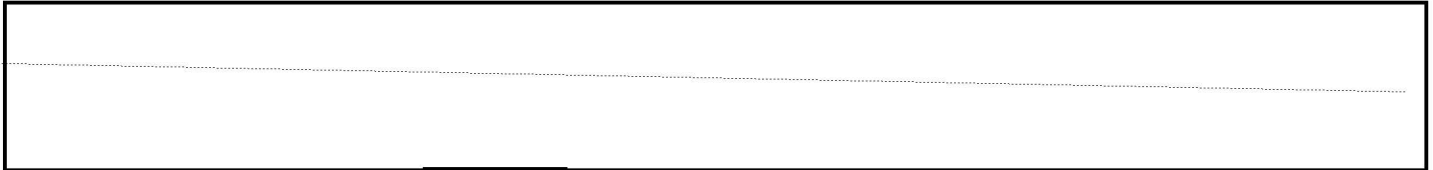
1. (U) Reviews of electronic communications or other documents containing FISA-acquired information that have been retained for further investigation and analysis or disseminated in accordance with these procedures.

(U) 2. ~~(S//NF)~~ Reviews of FISA-acquired information (from electronic surveillance and physical search) retained in electronic form to assess compliance with these procedures, including, with respect to raw FISA-acquired information in an electronic and data storage system that satisfies the requirements described in Sections III of these procedures, whether such raw FISA-acquired communications or property have been properly identified as information

that reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime. FISA-acquired communications and property may also be reviewed to determine whether they were

b1 -1
b3 -1
b7E -1,2

(S)



3. (U) Audits of [redacted] FISA-acquired information to assess the FBI's

compliance with the retention procedures for FISA-acquired information as detailed these procedures. The audits may also include reviewing a sampling of [redacted]

b7E -1,2

[redacted] and accesses to raw FISA-acquired information. These audits may assist in determining the FISA-acquired information that was accessed and the individuals who accessed the information. In turn, the minimization reviews may include verifying that the individuals who accessed the FISA-acquired information in FBI systems were individuals who had properly been given access under FBI guidelines.

B. (U) Training.

(U) The Attorney General, or a designee, shall ensure that adequate training on these procedures be provided to appropriate personnel.

C. (U) Minimization Briefings.

(U) Following the authorization of collection activity, an NSD attorney shall conduct a minimization briefing with appropriate FBI personnel responsible for the FISA surveillance or search.

VI. (U) INTERPRETATION

(U) The FBI shall refer all significant questions relating to the interpretation of these procedures to NSD.

VII. (U) REVIEW OF PROCEDURES

(U) The Attorney General, or a designee, in consultation with the FBI Office of General Counsel, shall review these procedures and determine whether they remain appropriate in light of the technology and practices used by the FBI no later than June 1, 2021, and every five years thereafter. A written report of such review shall be provided to the Court within six months of the completion of the review.



John P. Carlin
Assistant Attorney General for National Security

5-17-16
Date