Approved for public release as redacted by the ODNI 20160811

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
2015 JUL 15 PM 3:21
CLERK OF COURT

EXHIBIT D

MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF T[redacted] INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

TABLE OF CONTENTS

I. (U) GENERAL PROVISIONS 1

II. (U) ACQUISITION 4

A. ~~(S//NF)~~ Acquisition of [redacted] 4

III. (U) RETENTION 5

A. (U) Retention – Storage of FISA-acquired Information 5

B. (U) Retention – Access to FISA-acquired Information 6

C. (U) Retention – Review and Use of FISA-acquired Information 8

1. (U) General Provisions 8

2. (U) Sensitive Information 10

D. ~~(S//NF)~~ Retention – Queries of Electronic and Data Storage Systems Containing Raw FISA-acquired Information 11

E. ~~(S//NF)~~ Retention of Attorney-Client Communications 12

1. ~~(S//NF)~~ Target charged with a crime pursuant to the United States Code 13

2. ~~(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 15

3. ~~(S//NF)~~ Privileged communications involving targets and other persons not charged with a crime in the United States 17

F. (U) Additional Procedures for Retention, Use and Disclosure of FISA Information 19

~~Classified by: The Attorney General~~
~~Reason: 1.4(c)~~
~~Declassify on: 10 July 2040~~

Approved for public release as redacted by the ODNI 20160811

G. (U) Time Limits for Retention 22

1. [redacted]) Electronic and data storage systems other than those solely used for link analysis of metadata 22

a. ~~(S//NF)~~ FISA-acquired information that has been retained but not reviewed 22

b. ~~(S//NF)~~ FISA-acquired information that has been reviewed but not identified as meeting the applicable standard 23

2. ~~(S//NF)~~ Retention on media 23

3. ~~(S//NF)~~ Backup and evidence copies in FBI systems 24

4. ~~(S//NF)~~ Information retained in connection with litigation matters 24

5. ~~(S//NF)~~ Encrypted information 25

6. ~~(S//NF)~~ Retention of information in other forms 25

IV. (U) AD HOC DATABASES 25

A. ~~(S//NF)~~ Restrictions Concerning Access to and Identification of FISA-Acquired Information in an Ad Hoc Database 26

B. ~~(S//NF)~~ Restrictions Concerning Retention of FISA-Acquired Information in an Ad Hoc Database 27

C. ~~(S//NF)~~ Retention of FISA-Acquired Information that is Encrypted in an Ad Hoc Database 28

D. ~~(S//NF)~~ Analysis and Queries of Raw FISA-Acquired Information in an Ad Hoc Database 28

E. ~~(S//NF)~~ Procedures for Retention of Attorney-Client Communications in an Ad Hoc Database 29

V. (U) DISSEMINATION AND DISCLOSURE 30

A. (U) Dissemination of Foreign Intelligence Information to Federal, State, Local and Tribal Officials and Agencies 30

1. (U) Foreign Intelligence Information as defined in 50 U.S.C. § 1801(e)(1) 31

2. (U) Foreign Intelligence Information as defined in 50 U.S.C. § 1801(e)(2) 31

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) 31

C. (U) Dissemination to Foreign Governments 32

Approved for public release as redacted by the ODNI 20160811

D. ~~(S//NF)~~ Disclosure of Raw FISA-Acquired Information for Technical or Linguistic Assistance 33

E. ~~(S//NF)~~ Disclosure to the NSA and CIA 35

F. ~~(S//NF)~~ Dissemination of Foreign Intelligence Information for Terrorist Screening . 35

G. ~~(S//NF)~~ Disclosure to the National Counterterrorism Center (NCTC) of Information Acquired in Cases Related to Terrorism or Counterterrorism 35

H. ~~(S//NF)~~ Dissemination to Private Entities and Individuals of Foreign Intelligence Information or Evidence of a Crime Involving Computer Intrusion Events 36

I. ~~(S//NF)~~ Dissemination to Private Entities and Individuals of Foreign Intelligence Information or Evidence of a Crime Involving a Matter of Serious Harm 36

VI. (U) COMPLIANCE 37

A. (U) Oversight 37

B. (U) Training 39

VII. (U) INTERPRETATION 39

Approved for public release as redacted by the ODNI 20160811

I. (U) GENERAL PROVISIONS

A. (U) In accordance with 50 U.S.C. §§ 1801(h), 1821(4), and 1881a(c)(1)(A), these Federal Bureau of Investigation (FBI) minimization procedures govern the acquisition, retention, and dissemination of nonpublicly available information concerning unconsenting United States persons that is acquired by targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act"), 50 U.S.C. § 1881a. The Attorney General, in consultation with the Director of National Intelligence (DNI), has adopted these procedures after concluding that they meet the definition of minimization procedures under 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 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. (S//NF) For the purpose of these procedures:

1. the term "applicable FISA authority" refers to section 702 of the Act;

2. references to "information acquired pursuant to FISA" and "FISA-acquired information" will be understood to mean communications and information acquired pursuant to section 702 of the Act; and

Approved for public release as redacted by the ODNI 20160811

3. References to "target" will be understood to refer to the user(s) of a tasked facility.

C. ~~(S//NF)~~ Pursuant to 50 U.S.C. §§ 1806(a), no information acquired pursuant to FISA may be used or disclosed by Federal officers or employees except for lawful purposes. Information acquired pursuant to section 702 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. 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 the handling of information that is acquired in a manner inconsistent with certain of the limitations set forth in section 702(b), the use or disclosure of information as described in Section III.F.1. of these procedures, attorney-client communications, the use of FISA-acquired information in criminal proceedings in the United States and foreign countries, and the dissemination of raw FISA-acquired information to other agencies, these procedures do not apply to information concerning non-United States persons.

D. ~~(S//NF)~~ 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, 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 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

Approved for public release as redacted by the ODNI 20160811

belief that the individual is a United States person. 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.

E. (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. Any modification to these procedures must be made in accordance with 50 U.S.C. § 1881a(i)(1)(C).

F. (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 in accordance with 50 U.S.C. § 1881a(i)(1)(C), the FBI shall report that activity promptly to the NSD, which shall notify the Foreign Intelligence Surveillance Court (FISC) promptly of such activity.

G. ~~(S//NF)~~ 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, Office of the Director of National Intelligence (ODNI), or the applicable Offices of the Inspectors General. Additionally, nothing in these procedures shall prohibit the retention, processing, or dissemination of information reasonably necessary to comply with specific constitutional, judicial, or legislative mandates. Similarly, and notwithstanding any other section in these

Approved for public release as redacted by the ODNI 20160811

procedures, the FBI may use information acquired pursuant to section 702 of the Act to conduct security assessments of its systems in order to ensure that FBI systems have not been compromised. These security assessments may include, but will not be limited to, the temporary storage of section 702-acquired information in a separate system for a period not to exceed one year. While retained in such a storage system for security assessments, such section 702-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. ~~(S//NF)~~ Acquisition of [redacted].

1. ~~(S//NF)~~ The FBI may acquire [redacted] pursuant to section 702 of the Act only in accordance with FBI targeting procedures that have been adopted by the Attorney General, in consultation with the DNI, pursuant to section 702(d) of the Act.

2. ~~(S//NF)~~ As soon as FBI personnel recognize that an acquisition of a communication under section 702 of this Act is inconsistent with any of the limitations set forth in section 702(b),[1] the FBI will purge the communication and destroy all other copies of that

[1] (U) Subsection 702(b) provides that "[a]n authorization authorized under subsection (a) --

(1) may not intentionally target any person known at the time of the acquisition to be located in the United States;
(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be located in the United States;
(3) may not intentionally target a United States person reasonably believed to be located outside the United States;
(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States."

Approved for public release as redacted by the ODNI 20160811

communication that are accessible to any end user electronically or in hard copy. Any electronic copies of the communication that are not available to any end user but are available to a systems administrator as an archival back-up will be restricted and destroyed in accordance with normal business practices and will not be made available to any other person. In the event FBI archival back-up data is used to restore an electronic and data storage system, the FBI will ensure that the previously deleted communication will not be accessible to any user and will be deleted from any storage system.

III. (U) RETENTION

A. (U) Retention – Storage of FISA-acquired Information.

(U) The FBI must retain all FISA-acquired information under appropriately secure conditions that limit access to such information only to authorized users in accordance with these and other applicable FBI procedures. These retention procedures apply to FISA-acquired information retained in any form. FBI electronic and data storage systems may permit multiple authorized users to access the information simultaneously or sequentially and to share FISA-acquired information between systems.

~~(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 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. Illustrative examples of raw FISA-acquired information include audio recordings of intercepted communications (including copies thereof); soft or hard copies of e-mails [redacted]

Approved for public release as redacted by the ODNI 20160811

[redacted] digital images obtained [redacted] electronic storage media; verbatim translations of documents or communications; and intercepted communications that have been processed into the form of "tech cuts" but have not been evaluated to determine whether the tech cuts 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.

~~(S//NF)~~ Any communication acquired through the targeting of a person who at the time of targeting was reasonably believed to be a non-United States person located outside the United States but is in fact located inside the United States at the time such communication is acquired or is subsequently determined to be a United States person will be removed from FBI systems upon recognition, unless the Director or Deputy Director of the FBI specifically determines in writing on a communication-by-communication basis that such communication is reasonably believed to contain significant foreign intelligence information, evidence of a crime that has been, is being, or is about to be committed, or information retained for cryptanalytic, traffic analytic, or signal exploitation purposes. Notwithstanding the above, if any such communications indicate that a person targeted under section 702 has entered the United States, nothing in these procedures shall prevent the FBI from retaining and providing to the National Security Agency (NSA) and Central Intelligence Agency (CIA) technical information derived from such communication for collection avoidance purposes.

B. (U) Retention – Access to FISA-acquired Information.

~~(S//NF)~~ 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 will vary according to

Approved for public release as redacted by the ODNI 20160811

whether a particular storage system contains raw FISA-acquired information, will be consistent with the FBI's foreign intelligence information-gathering and information-sharing responsibilities, and shall include provisions:

1. 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;

2. Requiring the FBI to maintain accurate records of all persons to whom it has granted access;

3. Requiring the FBI to maintain accurate records of all persons who have accessed raw FISA-acquired information, and to audit its access records regularly to ensure that raw FISA-acquired information is only accessed by authorized individuals, including FBI personnel and the individuals referenced in Sections III.F and VI.A of these procedures;

4. Requiring training on these procedures and the FBI's policies regarding access to raw FISA-acquired information; and

5. Requiring the primary case agent(s) and his/her/their designees (hereinafter "case coordinator(s)") to control the marking of information in a particular case in accordance with FBI policy. A marking, for example, would include an indication that the information is or is not foreign intelligence.

~~(S//NF)~~ 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.

~~(S//NF)~~ 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

Approved for public release as redacted by the ODNI 20160811

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.

6. ~~(S//NF)~~ With respect to information acquired pursuant to section 702 of the Act, only those FBI personnel who have received training on the application of these "Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" may be designated as case coordinators. All FBI personnel having access to information acquired pursuant to section 702 of the Act will be informed of and provided access to these minimization procedures.

C. (U) Retention – Review and Use of FISA-acquired Information.

1. (U) General Provisions.

~~(S//NF)~~ FBI personnel with authorized access to raw FISA-acquired information may review, translate, analyze, and use all such information only in accordance with these procedures and FISA and only for the purpose of 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 determinations.

Approved for public release as redacted by the ODNI 20160811

~~(S//NF)~~ FBI personnel with authorized access may copy, transcribe, summarize, review, or analyze raw FISA-acquired information only as necessary to evaluate whether it 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. 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 or necessary to understand foreign intelligence may only be retained and disseminated for law enforcement purposes. The FBI shall identify FISA-acquired information in its storage systems, other than those used solely for link analysis of metadata, that has been reviewed and meets these standards.[2] If the FBI proposes to use any storage system that is incapable of meeting these requirements, the FBI shall follow the procedures set forth in Section I.E.

(U) Before using FISA-acquired information for 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.

(U) The FBI may disseminate copies, transcriptions, summaries, and other documents containing FISA-acquired information only in accordance with the dissemination procedures set forth in Section V below.

---

[2] ~~(S//NF)~~ Although the FBI need not mark metadata as meeting the retention standards or as having been disseminated, the FBI must still assess whether the metadata meets the requirements for dissemination pursuant to Section V prior to actually disseminating the information.

Approved for public release as redacted by the ODNI 20160811

~~(S//NF)~~ 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.

2. (U) Sensitive Information.

~~(S//NF)~~ 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:

(a) Religious activities of United States persons, including consultations with clergy;

(b) Educational and academic activities of United States persons, including consultations among professors or other teachers and their students;

(c) Political activities of United States persons, including discussions with Members of Congress and their staff, and other elected officials;

(d) Activities of United States persons involving the press and other media;

(e) Sexual and other highly personal activities of United States persons;

(f) Medical, psychiatric, or psychotherapeutic activities of United States persons; and

Approved for public release as redacted by the ODNI 20160811

(g) Matters pertaining to United States minor children, including student requests for information to aid in academic endeavors.

D. ~~(S//NF)~~ Retention – Queries of Electronic and Data Storage Systems Containing Raw FISA-acquired Information.

~~(S//NF)~~ Users who are authorized to have access to raw FISA-acquired information may query FBI electronic and data storage systems that contain raw FISA-acquired information 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. [redacted]

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.[3] Authorized users with access to raw FISA-acquired information may process the results of an appropriate query in accordance with Section III.C above. The FBI shall maintain records of all searches, including search terms, used by those with access to raw FISA-acquired information to query such systems. For purposes of this section, the term query does not include a user's search or query of an FBI electronic and data storage system that contains raw FISA-acquired information, where the user does not receive the raw FISA-acquired information in response to the search or query either because the user has not been granted

[3] ~~(S//NF)~~ It is a routine and encouraged practice for the FBI to query databases containing lawfully acquired information, including FISA-acquired information, in furtherance of the FBI's authorized intelligence and law enforcement activities, such as assessments, investigations and intelligence collection. Section III.D governs the conduct of such queries. Examples of such queries include, but are not limited to, queries reasonably designed to identify foreign intelligence information or evidence of a crime related to an ongoing authorized investigation or reasonably designed queries conducted by FBI personnel in making an initial decision to open an assessment concerning a threat to the national security, the prevention of or protection against a Federal crime, or the collection of foreign intelligence, as authorized by the Attorney General Guidelines. These examples are illustrative and neither expand nor restrict the scope of the queries authorized in the language above.

Approved for public release as redacted by the ODNI 20160811

access to the raw FISA-acquired information,[4] or because a user who has been granted such access has limited the query such that it cannot return raw FISA-acquired information.

~~(S//NF)~~ Users authorized to access FBI electronic and data storage systems that contain "metadata" may query such systems to find, extract, and analyze "metadata" pertaining to communications. The FBI may also use such metadata to analyze communications and may upload or transfer some or all such metadata to other FBI electronic and data storage systems for authorized foreign intelligence or law enforcement purposes. For purposes of these procedures, "metadata" is dialing, routing, addressing, or signaling information associated with a communication, but does not include information concerning the substance, purport, or meaning of the communication.

E. ~~(S//NF)~~ Retention of Attorney-Client Communications.

~~(S//NF)~~ This section governs the retention of attorney-client communications. The subparagraphs relating to attorney-client communications apply regardless of whether such communications are of or concerning U.S. persons. 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.

Approved for public release as redacted by the ODNI 20160811

1. ~~(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 NSD:

a. 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 [redacted] of a target who is charged with a crime pursuant to the United States Code;

[redacted] the FBI shall seal the original record or portion thereof containing that privileged communication, label it as containing privileged communications, forward the original record 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

Approved for public release as redacted by the ODNI 20160811

electronically to anyone other than system administrators or similar technical personnel. [redacted]

e. As soon as FBI personnel recognize that communications between the person under criminal charges and his attorney have been acquired [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, that user receives electronic notification that attorney-client communications have been acquired [redacted]

Approved for public release as redacted by the ODNI 20160811

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

2. ~~(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.

~~(S//NF)~~ 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. 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 will notify the Chief Division Counsel, FBI Office of General Counsel, and the 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 representing the individual in the criminal matter, the FBI shall implement procedures that include the following:

[redacted]

Approved for public release as redacted by the ODNI 20160811

[redacted]

[redacted] the FBI will 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. [redacted]

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

Approved for public release as redacted by the ODNI 20160811

[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, that user receives electronic notification that attorney-client communications have been acquired during the search or surveillance.[7] The purpose of the notification is to alert others who may review this information that they may encounter privileged communications.

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

[redacted] Such communications 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

[redacted]

Approved for public release as redacted by the ODNI 20160811

communication, consistent with the need to disseminate foreign intelligence information or evidence of a crime.

~~(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. [redacted]

~~(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]

Approved for public release as redacted by the ODNI 20160811

F. (U) Additional Procedures for Retention, Use and Disclosure of FISA Information.

1. ~~(S//NF)~~ In the event that the FBI seeks to use any information acquired pursuant to section 702 during a time period when there is uncertainty about the location of the target of the acquisition because the [redacted] post-tasking checks described in NSA's section 702 targeting procedures were not functioning properly, the FBI will follow its internal procedures for determining whether such information may be used (including, but not limited to, in FISA applications, section 702 targeting, and disseminations). Except as necessary to assess location under this provision, the FBI may not use or disclose any information acquired pursuant to section 702 during such time period unless the FBI determines, based on the totality of the circumstances, that the target is reasonably believed to have been located outside the United States at the time the information was acquired. If the FBI determines that the target is reasonably believed to have been located inside the United States at the time the information was acquired, such information will not be used and will be promptly destroyed.

2. ~~(S//NF)~~ Pursuant to 50 U.S.C. §§ 1806(b), no information acquired pursuant to section 702 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.

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

Approved for public release as redacted by the ODNI 20160811

understand foreign intelligence information or assess its importance, or to be evidence of a crime, are accessible when a search or query is conducted or made of FISA-acquired information.

4. (U) Prosecutors.

a. ~~(S//NF)~~ 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. ~~(S//NF)~~ 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.

c. ~~(S//NF)~~ The FBI may not provide federal prosecutors and others working at their direction with access to FBI electronic and data storage systems containing 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

Approved for public release as redacted by the ODNI 20160811

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 the FBI electronic and data and storage systems containing 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 must be requested from and approved by an executive at FBI Headquarters in a position no lower than Assistant Director (AD) 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;

iii. A request for access must specify to which FBI electronic and data and storage systems, FISC docket numbers and/or identifier of a certification executed by the DNI and Attorney General pursuant to section 702 of the Act (e.g., "DNI/AG 702(g) Certification [redacted] 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 direct access must receive user training on the system(s) to which they seek access, and training on the standard minimization procedures and any

Approved for public release as redacted by the ODNI 20160811

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 FBI electronic and data and storage systems containing 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 the NSD.

G. (U) Time Limits for Retention.

~~(S//NF)~~ 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. ~~(S//NF)~~ The FBI is authorized to retain data in electronic and data storage systems other than those solely used for link analysis of metadata, in accordance with the following:

a. ~~(S//NF)~~ <u>FISA-acquired information that has been retained but not reviewed.</u>

~~(S//NF)~~ FISA-acquired information that has been retained but never reviewed shall be destroyed five years from the expiration date of the certification authorizing the collection unless an AD, or one of his or her superiors, determines that an extension is necessary because the communications are reasonably believed to contain significant foreign intelligence information,

Approved for public release as redacted by the ODNI 20160811

or evidence of a crime that has been, is being, or is about to be committed. An extension under this paragraph may apply to a specific category of communications, and must be documented in writing, renewed on an annual basis, and promptly reported to the NSD and ODNI.

b. ~~(S//NF)~~ FISA-acquired information that has been reviewed but not identified as meeting the applicable standard.

~~(S//NF)~~ 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, may be retained and be fully accessible by authorized personnel for further review and analysis for [redacted] from the expiration date of the certification authorizing the collection. [redacted] from the expiration date of the certification authorizing the collection, access to such information contained in electronic and data storage systems will be limited to search capabilities that would produce notice to an authorized user that information responsive to a query exists. Approval from an AD, or AD's designee, is required to gain full access to this information.

~~(S//NF)~~ 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 [redacted] from the expiration date of the certification authorizing the collection unless specific authority is obtained from an AD and the 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."

[redacted]

Approved for public release as redacted by the ODNI 20160811

[redacted]

3. [redacted] **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 technical personnel have access to such information. 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. [redacted]

4. [redacted] **Information retained in connection with litigation matters**. The FBI may temporarily retain specific FISA-acquired information that would otherwise have to be destroyed under these procedures, [redacted]

Approved for public release as redacted by the ODNI 20160811

[redacted]

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.

[redacted]

IV. (U) AD HOC DATABASES

(U) Retention of Raw FISA-Acquired Information Outside of the Systems Described In Section III.

~~(S//NF)~~ If FBI personnel who are engaged in a particular investigation are unable to fully and completely review or analyze raw FISA-acquired information in an electronic and data storage system described in Section III of these procedures, the FBI may utilize electronic

Approved for public release as redacted by the ODNI 20160811

repositories other than the electronic and data storage systems described in Section III ("ad hoc databases") to review or analyze such information, provided that FBI's retention of raw FISA-acquired information in ad hoc databases occurs under appropriately secure conditions that limit access to such information to authorized personnel in accordance with the conditions set forth below. All FISA-acquired information maintained in ad hoc databases is subject to the Dissemination and Disclosure provisions in Section V and the Oversight provisions in Section VI. The subparagraphs relating to attorney-client privileged communications apply regardless of whether such communications are of or concerning U.S. persons. Except as otherwise provided below, all destruction requirements set forth in other sections of these procedures apply to any information maintained in an ad hoc database.

A. ~~(S//NF)~~ Restrictions Concerning Access to and Identification of FISA-Acquired Information in an Ad Hoc Database

1. ~~(S//NF)~~ Access to raw FISA-acquired information contained in an ad hoc database shall be limited to those individuals who are engaged in the particular investigation and those individuals who are conducting or aiding in the assessment or analysis of that information, as described in Section IV.B.1, C., or D. below. The FBI shall maintain a written or electronic record of employees who are granted access to the information while it is stored in an ad hoc database.

2. ~~(S//NF)~~ The FBI will identify FISA-acquired information in ad hoc databases in a manner that is sufficient to alert those who have access to the ad hoc database that it includes FISA-acquired information.

Approved for public release as redacted by the ODNI 20160811

B. ~~(S//NF)~~ Restrictions Concerning Retention of FISA-Acquired Information in an Ad Hoc Database

1. ~~(S//NF)~~ Raw FISA-acquired information concerning unconsenting U.S. persons may be placed in an ad hoc database 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. In addition, 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 database. FISA-acquired U.S. Person information in an ad hoc database that has been retained but not determined to be foreign intelligence information, necessary to understand foreign intelligence information or assess its importance, or evidence of a crime, shall be destroyed no later than five years from the expiration of the Certification authorizing the collection, unless an AD, or one of his superiors, determines that an extension is necessary to further analyze the information pursuant to this subparagraph. An extension under this subparagraph may apply to a specific category of communications, and must be documented in writing, renewed on an annual basis, and promptly reported to the NSD and ODNI.

2. ~~(S//NF)~~ The FBI will implement procedures regarding storage of FISA-acquired information in an ad hoc database, which will require the FBI to (1) maintain adequate records of all persons who have been granted access to FISA-acquired information in an ad hoc database, (2) track the FISA-acquired information in an ad hoc database 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) maintain adequate records to ensure FBI can comply with the destruction requirement discussed in subparagraph B.1. of this section.

Approved for public release as redacted by the ODNI 20160811

C. ~~(S//NF)~~ Retention of FISA-Acquired Information that is Encrypted in an Ad Hoc Database

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

D. ~~(S//NF)~~ Analysis and Queries of Raw FISA-Acquired Information in an Ad Hoc Database

~~(S//NF)~~ Users who are authorized to have access to raw FISA-acquired information in an ad hoc database 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.[8] The FBI's analytical techniques may include, but are not limited to, the use of

[redacted]

determined necessary by the FBI for the analysis of the data. FBI personnel must document the analytical and technical processes or techniques used to analyze data in an ad hoc database. Such documentation should reasonably identify the general nature of the manner in which the analysis of the information was conducted and tools employed during the analysis. If keyword searches are used to query data in an ad hoc database, such queries must be designed to find and

[8] ~~(S//NF)~~ Examples of such queries include, but are not limited to, queries reasonably designed to identify foreign intelligence information or evidence of a crime related to an ongoing authorized investigation or reasonably designed queries conducted by FBI personnel in making an initial decision to open an assessment concerning a threat to the national security, the prevention of or protection against a Federal crime, or the collection of foreign intelligence, as authorized by the Attorney General Guidelines. These examples are illustrative and neither expand nor restrict the scope of the queries authorized in the language above.

Approved for public release as redacted by the ODNI 20160811

extract foreign intelligence information or evidence of a crime. The FBI shall maintain either a written or electronic record of such keyword searches. [redacted]

E. ~~(S//NF)~~ Procedures for Retention of Attorney-Client Communications in an Ad Hoc Database

1. ~~(S//NF)~~ If FBI personnel discover attorney-client privileged communications in an ad hoc database [redacted] all such attorney-client privileged communications from the relevant Section 702 targeted facility must immediately be removed from the ad hoc database. To the extent that the ad hoc database is necessary to assess the remaining information acquired from the relevant Section 702 targeted facility to determine whether any of the information is attorney-client privileged [redacted] the FBI may retain the information in the ad hoc database for assessment by a review team until such determination has been made. Any attorney-client privileged communications [redacted] that are identified by the review team during this assessment will be removed from the ad hoc database. [redacted]. The review team will also notify anyone with access to the communications from the relevant 702 targeted facility that attorney-client privileged communications have been acquired and removed. To the extent that the attorney-client privileged communications from the relevant Section 702 targeted facility are accessible in an electronic and data storage system

Approved for public release as redacted by the ODNI 20160811

that has the marking, auditing and notification capabilities described in Section III, the FBI shall ensure it follows the provisions in [redacted]

[redacted]

3. (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.

V. (U) DISSEMINATION AND DISCLOSURE

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

~~(S//NF)~~ 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 V.A.1 and V.A.2 to federal, state, local and tribal officials and agencies with responsibilities relating to national security that require access

Approved for public release as redacted by the ODNI 20160811

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).

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

~~(S//NF)~~ 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.

~~(S//NF)~~ 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

Approved for public release as redacted by the ODNI 20160811

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.F.

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:

[redacted]

Approved for public release as redacted by the ODNI 20160811

[redacted]

3. ~~(S//NF)~~ The Attorney General, in consultation with the DNI or a designee, may authorize the use of information acquired or derived from an authorization under section 702 in a criminal proceeding conducted by a foreign government. 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. ~~(S//NF)~~ The FBI will make a written record of each dissemination approved pursuant to this section, and information regarding such disseminations and approvals shall be reported to the Attorney General, or a designee, on a quarterly basis.

D. ~~(S//NF)~~ Disclosure of Raw FISA-acquired Information for Technical or Linguistic Assistance.

~~(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 to assisting federal agencies for further processing and

Approved for public release as redacted by the ODNI 20160811

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, to NCMEC for further processing and analysis. The following restrictions apply with respect to any materials so disclosed:[9]

1. ~~(S//NF)~~ 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.

2. ~~(S//NF)~~ Disclosure will be only to those personnel within assisting federal agencies and 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.

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, 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.

4. ~~(S//NF)~~ Upon the conclusion of such technical assistance to the FBI, the FISA-acquired information or information disclosed to assisting federal agencies and NCMEC will

[9] (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.

Approved for public release as redacted by the ODNI 20160811

either be returned to the FBI or be destroyed, with an accounting of such destruction made to the FBI.

5. ~~(S//NF)~~ Any information that assisting federal agencies and 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.

E. ~~(S//NF)~~ Disclosure to the NSA and CIA.

~~(S//NF)~~ With respect to any communications that the FBI acquires from an electronic communication service provider pursuant to section 702 of the Act, the FBI may convey such communications to the NSA and CIA in unminimized form. The NSA and CIA shall handle any [redacted] received from the FBI pursuant to these procedures in accordance with the NSA and CIA minimization procedures, respectively, adopted by the Attorney General, in consultation with the DNI, pursuant to section 702(e) of the Act.

F. ~~(S//NF)~~ Dissemination of Foreign Intelligence Information for Terrorist Screening.

~~(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.

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

~~(S//NF)~~ In addition to other disclosures permitted in these procedures, the FBI may provide to NCTC information in FBI general indices, including the Automated Case Support

Approved for public release as redacted by the ODNI 20160811

(ACS) system, Sentinel, or 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 this section is contingent upon NCTC's application of the NCTC section 702 minimization procedures approved by the FISC with respect to such information. 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.

H. ~~(S//NF)~~ Dissemination to Private Entities and Individuals of Foreign Intelligence Information or Evidence of a Crime Involving Computer Intrusion Events.

~~(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. ~~(S//NF)~~ Dissemination to Private Entities and Individuals of Foreign Intelligence Information or Evidence of a Crime Involving a Matter of Serious Harm.

~~(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

Approved for public release as redacted by the ODNI 20160811

where the FBI determines that said private individual or entity is capable of providing assistance in mitigating 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 subsequently report to the FISC any disseminations made pursuant to this paragraph.

VI. (U) COMPLIANCE

A. (U) Oversight.

~~(S//NF)~~ 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.F 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.

~~(S//NF)~~ 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:

Approved for public release as redacted by the ODNI 20160811

1. ~~(S//NF)~~ 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.

2. ~~(S//NF)~~ Reviews of FISA-acquired information in FBI electronic and data storage systems that contain raw FISA-acquired information to assess compliance with these procedures, including whether raw FISA-acquired communications or property have been properly marked 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 in FBI electronic and data storage systems that contain raw FISA-acquired information may also be reviewed to determine whether they were [redacted].

3. ~~(S//NF)~~ Audits of queries in FBI electronic and data storage systems containing raw FISA-acquired information to assess the FBI's compliance with the retention procedures for FISA-acquired information as detailed in Section III of these procedures. The audits may also include reviewing a sampling of logs or other records that list FBI analysts and agents and their queries and accesses in FBI electronic and data storage systems containing raw FISA-acquired information. These audits may assist in determining the FISA-acquired information that was accessed in these FBI electronic and data storage systems 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 these FBI systems were individuals who had properly been given access under FBI guidelines.

Approved for public release as redacted by the ODNI 20160811

B. (U) **Training.**

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

VII. (U) INTERPRETATION

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

JUL 10 2015
Date

Loretta E. Lynch
Attorney General of the United States