~~SECRET//NOFORN~~

(U) EXHIBIT D

(U) 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

FILED UNDER SEAL

~~Classified by: The Deputy Attorney General~~
~~Derived from: DOJ/NSI SCG-1, 1.6, FBI NSICG INV~~
~~Declassify on: 20461018~~

(U) **TABLE OF CONTENTS**

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 requirements 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. § 3024(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. These minimization procedures apply in addition to separate querying procedures adopted pursuant to subsection 702(f)(1) of the Act. These minimization procedures should be read and applied in conjunction with those querying procedures, and nothing in these procedures permits any actions that would otherwise be prohibited by those querying procedures.

B. (U) 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

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

C. (U) 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.H.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 disclosure of raw FISA-acquired information to other agencies, these procedures do not apply to information concerning non-United States persons.

D. (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, 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 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. A person known to have been at any time an alien admitted for lawful permanent residence is treated as a United States person, unless a determination that such person is no longer a United States person is made (a) in consultation with the FBI Office of General Counsel after obtaining a copy of either an order revoking that person's United States person status issued by a U.S. federal court or a properly executed and filed United States Citizenship and Immigration Services Form I-407 (Record of Abandonment of Lawful Permanent Resident Status), or (b) in consultation with the FBI Office of General Counsel and the National Security Division (NSD) of the Department of Justice.

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 NSD's Office of Intelligence to request that these procedures be modified. Any modification to these procedures must be made in accordance with 50 U.S.C. § 1881a(j)(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(j)(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. (U) Nothing in these procedures[1] shall restrict the lawful oversight functions of the NSD, Office of the Director of National Intelligence (ODNI), or the applicable Offices of the Inspectors General or restrict FBI from providing the assistance necessary for these entities to perform their lawful oversight functions. Notwithstanding the access and review restrictions in Sections III.A.1 and III.C.1.a of these procedures,[2] respectively, FBI personnel who are undergoing, but have not yet completed, training regarding the proper implementation of FISA and the FBI's FISA procedures, including its section 702 procedures, may have access to and review raw section 702-acquired information during the conduct of such training to the extent reasonably necessary for the training to be effective.[3] The review restrictions in Section III.C.1.a of these procedures shall not restrict the FBI's ability to perform activities necessary to create,

[1] (U) Whenever relying on any portion of Section I.G. of these procedures to deviate from any provision of these minimization procedures, FBI personnel shall limit the scope of their deviation and comport with all other provisions of these minimization procedures to the maximum extent practicable.

[2] (U) Specifically, as provided in III.A.1, "FBI personnel with access to raw FISA-acquired information must receive training on these minimization procedures before receiving access to raw FISA-acquired information." And, as provided in III.C.1.a, FBI may make raw FISA-acquired information available to authorized personnel on a continuing basis … 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." As further provided in III.C.1.a, "FBI personnel with authorized access to raw FISA-acquired information may review, translate, copy, transcribe, analyze, summarize, and use all such information … 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."

[3] (U) Although the access and review restrictions in Section III of these procedures do not restrict the FBI's ability to perform lawful training functions of its personnel regarding the proper implementation of provisions of FISA other than section 702, these procedures do not authorize such training. The minimization procedures applicable to collection acquired pursuant to provisions of FISA other than section 702 dictate whether such training is permitted.

test, or conduct technical maintenance of the functions of FBI systems that process or store section 702-acquired information. Additionally, nothing in these procedures shall prohibit the retention, processing, analysis, or dissemination of information necessary to comply with an order of a court within the United States or a specific congressional mandate, such as a subpoena or other similar process consistent with congressional oversight. Similarly, and notwithstanding any other section in these 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 are not limited to, the temporary retention of section 702-acquired information in a separate system for a period not to exceed one year. While retained in such a 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.

H. ~~(S//NF)~~ Nothing in these procedures[4] shall restrict the FBI's ability to review section 702-acquired information that FBI determines is necessary to remediate a potential spill of section 702-acquired information. In addition, nothing in these procedures shall restrict the FBI's ability to review, retain, and disclose section 702-acquired information that FBI determines is necessary to support FBI's investigation and remediation of a possible FISA compliance incident or FBI's activities necessary to identify section 702-acquired information subject to destruction, including under these minimization procedures. [redacted]

[redacted]

[4] (U) Whenever relying on any portion of Section I.H. of these procedures to deviate from any provision of these minimization procedures, FBI personnel shall limit the scope of their deviation and comport with all other provisions of these minimization procedures to the maximum extent practicable.

[redacted] Should the FBI determine it is necessary to deviate from an aspect of these minimization procedures to perform lawful oversight functions of its personnel or systems apart from the exceptions described above in this section (I.H.), the FBI shall consult with NSD and ODNI prior to conducting such activity. NSD shall promptly report the deviation to the FISC. Each such report shall describe the nature of the deviation from the procedures and identify the specific oversight activity for which the deviation was necessary. Once section 702-acquired information is no longer reasonably believed to be necessary for a lawful oversight function, the information shall be destroyed to the extent required by 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. (U) As soon as FBI personnel recognize that an acquisition of information under section 702 of this Act is inconsistent with any of the limitations set forth in section 702(b),[5] the

[5] (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;

FBI will purge the information and destroy all other copies of that information that are accessible to any end user electronically or in hard copy. Any electronic copies of the information 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 information will not be accessible to any user and will be deleted from any storage system.

3. (U) Any communications acquired pursuant to section 702 that contain a reference to, but are not to or from, a person targeted in accordance with section 702 targeting procedures are unauthorized acquisitions and therefore will be destroyed upon recognition.[6]

III. (U) RETENTION

A. (U) **General.** Except where indicated below, these retention provisions apply to FISA-acquired information the 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

---

(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;
(5) may not intentionally acquire communications that contain a reference to, but are not to or from a target of an acquisition authorized under subsection (a), except as provided under section 103(b) of the FISA Amendments Reauthorization Act of 2017; and
(6) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States."

[6] (U) In applying this provision, note that any user of a tasked facility is regarded as a person targeted for acquisition.

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.

2. [redacted]

3. (U) Any information 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 information 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 that each specific item of acquired information to be retained 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 information indicates that a person targeted under section 702 has entered the United States, nothing in these procedures

[7] [redacted]

[8] [redacted]

shall prevent the FBI from retaining and providing to the National Security Agency (NSA), Central Intelligence Agency (CIA), or National Counterterrorism Center (NCTC) technical information derived from such information for collection avoidance purposes.

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

1. (U) "FISA-acquired information" means all information that the FBI acquires from an acquisition conducted pursuant to section 702 of FISA.

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. Illustrative examples of raw FISA-acquired information include audio recordings of intercepted communications (including copies thereof); soft or hard copies of e-mails [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. 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 information, to be necessary to understand foreign intelligence information or to assess its importance, or to be evidence of a crime.

3. (U) An "electronic and data storage system" is any FBI application, program, device, or process that retains or provides access to raw FISA-acquired information in electronic

form and meets the requirements in Sections III.C and III.D. An electronic and data storage system may reside on a server or network or may consist of a single stand-alone terminal or device. The FBI shall maintain and make widely available within FBI and to NSD a current list of all systems deemed to be electronic and data storage systems.

4. (U) 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. An ad hoc system may reside on a server or network or may consist of a single stand-alone terminal or device.

5. (U) "Query" means the use of one or more terms[9] to retrieve the unminimized contents or noncontents (including metadata) of section 702-acquired information that is located in a covered agency's system. The term "query" does not include a user's query of a system that contains unminimized section 702-acquired information, where the user does not receive unminimized section 702-acquired information in response to the query either because the user has not been granted access to the unminimized section 702-acquired information, or because a user who has been granted such access has limited the query such that it cannot retrieve unminimized section 702-acquired information. The term "query" also does not include (1) a

[9] ~~(S//NF)~~ Such terms may include the use of keywords, identifiers, [redacted].

system user's actions subsequent to conducting a query for purposes of sorting the results of that query based upon the attributes of the information retrieved,[10] or (2) examining or manipulating, including by technical means, communications or documents for the purpose of minimizing such communications or documents.[11]

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

[10] (U) For example, the action of a system user to sort the results of a query (i.e., the information actually returned to a system user from a query) by date, time, etc.

[11] (U) For example, an analyst might run a script against a spreadsheet that would find and replace all instances of a known United States person's name with a generic term, such a "U.S. Person 1."

evidence of a crime. Such personnel shall exercise reasonable judgment in making such evaluations or determinations.

(U) With respect to information acquired pursuant to section 702 of the Act, only those FBI personnel who have received training on these minimization procedures 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.

b. (U) *Information meeting criteria*. Once FBI personnel have assessed that raw FISA-acquired information 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, 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 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. However, when FBI transfers or copies FISA-acquired information from an electronic and data storage system, ad hoc system, or system used for transitory retention onto a medium, device, or system that is not an electronic and data storage system or ad hoc system as defined by these procedures, any information of or concerning a U.S. person, including that person's identity, that is being transferred that does not meet the retention standard (i.e., 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) must be stricken or a substitution made prior to the transfer.

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 Section 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.

f. (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:

(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

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

2. (U) Procedures Regarding Access to FISA-acquired Information Retained in Electronic Form.

(U) 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, 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.4 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. Queries of unminimized information acquired in accordance with section 702 of the Act are governed by the Querying Procedures Used in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended ("Querying Procedures"). All such queries conducted by FBI personnel must be made in accordance with those procedures. Authorized FBI users with access to raw section 702-acquired information must process the results of an appropriate query of raw section 702-acquired information in accordance with these minimization procedures.

4. (U) Retention Time Limits. The FBI is authorized to retain data in electronic and data storage systems, in accordance with the following:

a. (U) *Standard for retention.* These procedures do not limit the retention of 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.

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 certification authorizing the collection unless an executive at FBI Headquarters in a position no lower than an Assistant Director (AD) determines that an extension is necessary because the information is reasonably believed to contain significant foreign intelligence information, 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 information, and must be documented in writing, renewed on an annual basis, and promptly reported to ODNI and NSD, which will promptly notify the FISC in writing of all such determinations.

c. (U) *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 10 years from the expiration date of the certification authorizing the collection. Ten years from the expiration date of the certification 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 an AD, or such person's designee, is required to gain full access to this information.

(U) 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, shall be destroyed 15 years 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."

5. (U) Retention of Attorney-Client Communications.

(U) This section governs the retention of attorney-client communications in electronic and data storage systems. 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.

a. (U) *Target charged with a crime pursuant to the United States Code.*

(U) 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:

i. (U) 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 an acquisition of a target who is charged with a crime pursuant to the United States Code;

ii. [redacted]

iii. ~~(S//NF)~~ [redacted] 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 electronically to anyone other than system administrators or similar technical personnel.

iv. [redacted]

[redacted]

vi. (U) As soon as FBI personnel recognize that communications between the person under criminal charges and his attorney have been acquired pursuant to an acquisition under section 702, the FBI shall ensure that whenever any user reviews information or communications acquired from that acquisition, 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 acquisition.[12] The purpose of the notification is to alert others who may review this information that they may encounter privileged communications.[13]

b. (U) *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.*

(U) 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

[12] [redacted]

[13] [redacted]

(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) 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, or property is charged with a crime in the United States, they shall 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] 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

[14] ~~(S//NF)~~ If raw FISA-acquired information from the acquisition is also contained in an ad hoc system, described below, the FBI shall ensure that users with access to such information are similarly notified. Such notice shall comply with the rules for ad hoc systems, set forth at Section III.E.

electronically to anyone other than system administrators or similar technical personnel;

[redacted]

v. (U) As soon as FBI personnel recognize that communications between the person under criminal charges and his attorney have been acquired pursuant to a particular section 702 acquisition, the FBI shall ensure that whenever any user reviews information or communications acquired from that acquisition, 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 acquisition. The purpose of the notification is to alert others who may review this information that they may encounter privileged communications.[15]

c. (U) *Privileged communications involving targets and other persons not charged with a crime in the United States.*

[redacted]

15 [redacted]

[redacted]

(U) 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 the 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) 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, Deputy Attorney General, or the Assistant Attorney General for National Security. All such disseminations outside the United States Intelligence Community shall be limited to the greatest extent practicable and shall be consistent with policies and procedures issued by the Department of Justice that are designed to protect any applicable privilege.

(U) 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, Deputy Attorney General, or the Assistant Attorney General for National Security.

(U) If the FBI determines that a privileged FISA-acquired communication of a person not charged with a crime in the United States is not foreign intelligence information but is evidence of a crime, the FBI must obtain approval to disseminate the information for law enforcement purposes from the Attorney General, Deputy Attorney General, or the Assistant Attorney General for National Security. The FBI may disseminate the information immediately if it determines there is an immediate threat to life or of serious property damage. If the FBI makes such a dissemination, it shall immediately inform the NSD.

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) 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. If the ad hoc system that FBI personnel determine they may use is not capable of generating electronic records of queries, then their determination that they may use the ad hoc system for review or analysis also serves as their determination that they may conduct queries in that system, as described in paragraph IV of the Querying Procedures.

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

(U) 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. 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 system.

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.

c. (U) 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 certification authorizing the collection, unless specific authority is obtained from an executive at FBI Headquarters in a position no lower than an AD who 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, which will promptly notify the FISC in writing of all such determinations.

d. (U) The FBI will keep records that (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 (iii) document the removal of FISA-aequired information as required in Section III.E.4.c

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

(U) Queries of raw information acquired in accordance with section 702 of the Act are governed by the Querying Procedures. All such queries conducted by FBI personnel in ad hoc systems, and the handling of results of sueh queries, must be in accordance with the relevant provisions of those Querying Procedures and these minimization procedures.

6. (U) Procedures for Retention of Attorney-Client Communications.

a. (U) If FBI personnel discover attorney-client privileged communications in an ad hoc system that fall within Section III.D.5.a or III.D.5.b, all such attorney-client privileged communications from the relevant section 702-targeted facility must immediately be removed from the ad hoc system.

i. (U) To the extent that the ad hoc system 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 pursuant to Section III.D.5.a or III.D.5.b, the FBI may retain the information in the ad hoc system for assessment by a review team of one or more monitors and/or reviewers, who have no role in the prosecution of the charged criminal matter, until such determination has been made.

ii. (U) Any attorney-client privileged communications that fall within Section III.D.5.a or III.D.5.b that are identified by the review team during this assessment shall be removed from the ad hoc system. Any remaining communications not subject to Section III.D.5.a or III.D.5.b may be retained in an ad hoc system and shall be subject to the provisions in this section.

iii. (U) The review team shall also notify anyone with access in the ad hoc system to the communications from the relevant section 702- targeted facility that attorney-client privileged communications have been acquired and removed.

iv. (U) To the extent that the attorney-client privileged communications from the relevant section 702-targeted facility are also accessible in an electronic and data storage system, the FBI shall ensure it follows the provisions in Section III.D.5.a or III.D.5.b for those copies of the attorney-client privileged communications.

b. (U) If the FBI identifies attorney-client privileged communications that are determined to fall within Section III.D.5.c, the FBI may retain such communications in an ad hoc system pursuant to the provisions in this Section.

i. (U) The FBI shall notify anyone with access to the communications in the ad hoc system that attorney-client privileged information from the relevant section 702-targeted facility has been acquired and identify the

particular communications that are privileged pursuant to Section III.D.5.c.
ii. (U) 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, the FBI shall ensure it follows the provisions in Section III.D.5.c for those attorney-client privileged communications.

(U) For any dissemination of an attorney-client privileged communication retained in an ad hoc system that is determined to fall within Section III.D.5.c, the FBI shall ensure it follows the dissemination provisions in Section III.D.5.c for those attorney-client privileged communications.

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.

F. (U) **Special Purpose Systems**[16]

1. (U) **Collection Platforms**. Collection platforms include those platforms or systems that are used to enable or facilitate the acquisition, validation, or processing of raw FISA-acquired information or send collected information to other systems for review and analysis. In order for a collection platform to be exempt from Sections III.C, III.D, and III.E, (i) access to raw FISA-acquired information on the platform or system must be limited to system administrators or other similar technical personnel to perform their official duties, and (ii) no analytical work may be performed in the collection platform, nor may the data be accessed within the collection platform for the purpose of performing intelligence analysis. Raw FISA-acquired information shall not be retained in a collection system longer than one year from the expiration of the certification authorizing the collection.

[16] (U) Nothing in these Procedures permits the retention of information obtained through unauthorized acquisitions.

2. (U) **Systems Used Solely for Audits and Oversight**. Audit and oversight systems include those systems solely used for audits or quality-control reviews. For an audit and oversight system to be exempt from Sections III.C, III.D, and III.E, (i) access to the system must be limited to system administrators or other similar technical personnel, language services personnel, inspection personnel, and internal oversight/audit personnel, (ii) personnel with access to the system must limit the scope of their access to those activities necessary to perform their official duties, and (iii) no analytical work may be performed in such systems, nor may the data be accessed within such systems for the purpose of performing intelligence analysis. Raw FISA-acquired information shall not be retained in an audit and oversight system longer than one year from the expiration of the certification authorizing the collection.

[redacted]

[redacted]

~~(S//NF)~~ In the event that FBI recognizes section 702-acquired information in a record stored in a system subject to the requirements of this section and such information meets the retention requirement(s) in these procedures and is not otherwise subject to purge, FBI may retain such record. If FBI determines that the record does not otherwise meet the criteria for indefinite retention or the record is subject to purge, it will delete the record unless it is necessary to retain for the purposes served by this system. In the event FBI retains a record that contains section 702-acquired information that does not meet the applicable retention standard in these procedures or is otherwise subject to purge, the government shall report such retention in its next quarterly report concerning compliance matters under section 702 and include the reason retention of the information in that system is necessary for the purposes served by the system. Once FBI determines that it is no longer necessary to retain the raw section 702-acquired information for such purposes, the information shall be destroyed if subject to purge or to the extent required by the applicable provisions of these procedures.

[redacted]

[redacted]

~~(S//NF)~~ In the event that FBI recognizes section 702-acquired information in a record stored in a system subject to the requirements of this section and such information meets the retention requirement(s) in these procedures and is not otherwise subject to purge, FBI may retain such record. If FBI determines that the record does not otherwise meet the criteria for indefinite retention or is otherwise subject to purge, it will delete the record unless it is necessary to retain for the purposes served by this system. In the event FBI retains a record that contains section 702-acquired information that does not meet the applicable retention standard in these procedures or is otherwise subject to purge, the government shall report such retention in its next quarterly report concerning compliance matters under section 702 and include the reason retention of the information in that system is necessary for the purposes served by the system. Once FBI determines that it is no longer necessary to retain the section 702-acquired information

for such purposes, the information shall be destroyed if subject to purge or to the extent required by the applicable provisions of these procedures.

7. ~~(S//NF)~~ **Systems or Other Repositories That Contain Data Obtained Through User Activity Monitoring Activities.** The FBI conducts user activity monitoring ("UAM") activities, which are activities designed to provide the FBI with the technical capability to observe and record the actions and activities of a user on an FBI device or network in order to detect insider threats and support authorized investigations of such users. Insofar as FBI's UAM activities capture records that contain raw section 702-acquired information, such information may be contained in an FBI system or other repository provided that the retention of such information is in furtherance of an authorized use specified in this paragraph. Records captured by FBI's UAM activities that contain raw section 702-acquired information shall not be subject to the requirements of sections III.C, III.D, III.E, III.F.4, and III.I.3-4 of these procedures. Access to records captured by FBI's UAM activities that contain raw section 702-acquired information shall be limited to FBI personnel who require access to perform their official duties related to an authorized use specified in this paragraph, [redacted] Any personnel with access to records captured by FBI's UAM activities that contain raw section 702-acquired information must receive training on these procedures. FBI personnel who have access to records captured by FBI's UAM activities that contain raw section 702-acquired information may use such records to also assist in insider threat inquiries or investigations; security inquires and investigations regarding the eligibility of FBI personnel to access classified information or hold a sensitive position; counterintelligence inquiries and investigations, [redacted]

[redacted] The FBI shall maintain records of all personnel who have access to records captured by FBI's UAM activities that contain raw section 702-acquired information. Any dissemination of records captured by FBI's UAM activities that contain raw section 702-acquired information must be made in accordance with the dissemination requirements in these procedures.

~~(S//NF)~~ In the event that the FBI recognizes a record captured by FBI's UAM activities that contains section 702-acquired information and such information meets the retention requirement(s) in these procedures and it is not otherwise subject to purge, the FBI may retain such record. If the FBI determines that the record does not otherwise meet the criteria for retention, it will delete the record unless it is necessary to retain in furtherance of an authorized use specified in this paragraph. In the event the FBI retains a record that contains section 702-acquired information that does not meet the applicable retention standard or is otherwise subject to purge, the government shall report such retention in its next quarterly report concerning compliance matters under section 702 and include the reason why it is necessary to retain the information in furtherance of an authorized use specified in this paragraph. Once the FBI determines that it is no longer necessary to retain the section 702-acquired information in furtherance of an authorized use specified in this paragraph, the information shall be destroyed to the extent required by the applicable provisions of these procedures or other requirements.

8. (U) **Backup and Evidence Copies in FBI Systems**. The FBI may retain on a system emergency backup or original evidence copies of information in accordance with the restrictions set forth in Section III.I.2.

9. (U) **Queries in Special Purpose Systems.** Any queries conducted in special purpose systems, other than those systems described in Sections III.F.5-7, must be conducted in accordance with the Querying Procedures.

G. (U) **Metadata**

[redacted]

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

1. (U) 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

[redacted]

acquisition because the technical 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. (U) 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. (U) 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 search or query is conducted or made of FISA-acquired information.

4. (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.

c. (U) 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. (U) 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. (U) 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 and Cyber Law Branch or a Senior Executive Service attorney in the National Security and Cyber Law Branch, and will be considered on a case-by-case basis. Access to raw FISA-acquired information in any other form 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 and Cyber Law Branch, and will be considered on a case-by-case basis;

iii. ~~(S//NF)~~ A request for access must specify to which FBI electronic and data and storage system or ad hoc system, 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(h) Certification 2018-A"), and targeted facilities the prosecutor needs access, why such access is necessary, and the duration of such access;

iv. (U) 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 relevant FBI minimization procedures and any relevant supplemental minimization procedures applicable to the information to which they have access;

v. (U) Access shall be terminated no later than the conclusion of the relevant investigation or prosecution; and

vi. (U) 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 the NSD.

I. (U) **Other Time Limits for Retention.** In general, the FBI may retain section 702-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. (U) Retention on media. Five years from the expiration date of the certification authorizing the collection, access to information that is retained on electronic storage media as an original or evidentiary copy of FISA-acquired information, but not connected to or accessible through an electronic and data storage system or ad hoc system, shall be restricted. Thereafter, access to such information shall be granted only on a case-by-case basis upon the authorization of a section chief of the FBI and consultation with NSD. The original or evidentiary copy of FISA-acquired information retained under this subsection shall be destroyed in accordance with FBI policy.

2. (U) 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. Emergency backup or original evidence copies of information retained on a system are otherwise exempt from all of Sections III.C, III.D, and III.E. The original or

evidentiary copy of FISA-acquired information retained under this subsection shall be destroyed in accordance with FBI policy.

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

[redacted]

4. (U) 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. Once information is decrypted or the secret meaning is revealed, the retention time periods described in Section III.D.4 or III.E.4, as appropriate, shall be calculated as of the date of decryption, if that date is later than the expiration of the certification pursuant to which the information was acquired.

5. (U) Retention of information in other forms. 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

(U) Nothing in these procedures authorizes the dissemination of non-publicly available information that identifies any United States person without such person's consent unless: (1) such person's identity is necessary to understand foreign intelligence information or assess its importance; (2) the information is foreign intelligence information as defined in 50 U.S.C. § 1801(e)(1); or (3) the information is evidence of a crime which has been, is being, or is about to be committed and that is to be disseminated for law enforcement purposes.

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.H.

C. (U) Dissemination to Foreign Governments.

(U) 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]

[redacted] the FBI shall undertake reasonable steps to ensure that the disseminated

information will be used in a manner consistent with United States laws, including Executive Order 12333 (as amended) and applicable federal criminal statutes.

3. (U) 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. (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 reported to the Attorney General, or a designee, on a quarterly basis.

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

(U) 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 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:[19]

[19] (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.

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.

2. (U) 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. (U) 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. (U) Upon the conclusion of such technical assistance to the FBI, the FISA-acquired information or information 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.

E. (U) Disclosure to the NSA, CIA, and NCTC.

~~(S//NF)~~ With respect to any information that the FBI acquires from an electronic communication service provider pursuant to section 702 of the Act, the FBI may convey such information to the NSA and CIA in unminimized form. With respect to any information that the FBI acquires from an electronic communication service provider pursuant to DNI/AG 702 Certifications [redacted] the FBI may convey such information to the NCTC in unminimized form. The NSA, CIA, and NCTC shall handle any [redacted] received from the FBI pursuant to these procedures in accordance with the minimization and querying procedures for those respective agencies, adopted by the Attorney General, in consultation with the DNI, pursuant to subsections 702(e) and 702(f)(1) of the Act, respectively.

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

(U) 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. (U) Disclosure to NCTC of Information Acquired in Cases Related to Terrorism or Counterterrorism.

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

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

(U) 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.

2. (U) Reviews of FISA-acquired information 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 Section III of these procedures, whether such raw FISA-acquired information has 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 information may also be reviewed to determine whether it was properly identified pursuant to the attorney-client communications provisions of these procedures.

3. (U) Audits of queries of raw FISA-acquired information to assess the FBI's compliance with the provisions detailed in the Querying Procedures. The audits may include reviewing a sampling of logs or other records that list FBI analysts and agents and their queries and accesses to raw FISA-acquired information. These audits may assist in determining FBI's compliance with the procedures set forth in subsection 702(f)(2) of FISA and the requirement that the government report to the FISC each instance after December 4, 2015, in which FBI personnel received and reviewed Section 702-acquired information that FBI identified as concerning a United States person in response to a query that was not designed to find and extract foreign intelligence information. These audits may also 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.

VI. (U) INTERPRETATION

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

10/14/21
Date

Lisa Monaco
LISA O. MONACO
Deputy Attorney General of the United States