~~SECRET//NOFORN~~

(U) **EXHIBIT D**

(U) ~~(S//NF)~~ MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION CONCERNING THE INTERNATIONAL PRODUCTION, DISTRIBUTION, OR FINANCING OF CERTAIN ILLICIT DRUGS PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

1. (U) GENERAL PROVISIONS

A. ~~(S//NF)~~ 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 any certification entitled "In the Matter of [redacted] executed 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

FILED UNDER SEAL

~~Classified by: The Assistant Attorney General for National Security~~
~~Derived from: DOJ/NSI SCG-1, 1.6, FBI NSICG INV~~
~~Declassify on: 20491216~~

~~SECRET//NOFORN~~

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 national 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. ~~(S//NF)~~ References to "information acquired pursuant to FISA," "FISA-acquired information," "acquired pursuant to FISA," and "section 702-acquired information" will be understood to mean communications and information acquired pursuant to section 702 of the Act under a certification entitled "In the Matter of [redacted]

2. (U) ~~(S//NF)~~ "Raw FISA-acquired information" is FISA-acquired information that is in the same or substantially same format as when the FBI acquired it. 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) "Query" means the use of one or more terms[1] to retrieve the unminimized contents or noncontents (including metadata) of section 702-acquired information that is located in a covered agency's system; and

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

~~SECRET//NOFORN~~

4. (U) 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 acquisition requirements in Section II.A, the access and review restrictions set forth in Sections III.A.2 and III.A.4, 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:

1. (U) A person known to be located in the United States will be presumed to be a United States person unless identified as an alien who has not been admitted for permanent residence or the circumstances otherwise give rise to a reasonable belief that such person is not a United States person.

2. (U) A person known to be located outside the United States or whose location is not known will be presumed to be a non-United States person unless such person is identified as

a United States person, or the circumstances otherwise give rise to a reasonable belief that such person is a United States person.

3. (U) A person known to have been at any time an alien admitted for lawful permanent residence will be presumed to be 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. A person known to have been at any time a citizen of the United States will be presumed to be a United States person, unless a determination that such person is no longer a United States person is made in consultation with the FBI Office of General Counsel and NSD.

4. (U) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless the circumstances otherwise give rise to a reasonable belief that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence.

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[2] 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 Section III.A.1 of these procedures,[3] FBI technical and oversight 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.[4] Nothing in these procedures shall restrict the FBI's ability to perform activities necessary to create, test, or conduct technical maintenance of the functions of FBI technical systems that process or store section 702-acquired information.

---

[2] (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.

(U) [3] ~~(S//NF)~~ 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."

[4] (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.

~~SECRET//NOFORN~~

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[5] 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] 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

[5] (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.

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)~~ Although the FBI may not retain or use FISA-acquired information for any operational or analytical purpose (unless otherwise provided for herein in support of network security assessments or User Activity Monitoring activities), the FBI may acquire [redacted] pursuant to section 702 of the Act only in accordance with the 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),[6] the

[6] (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;

FBI will purge the information. Any electronic copies of the section 702-acquired information that are available to a systems administrator as an archival back-up[7] 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 a collection platform, the FBI will ensure that the previously deleted information will not be accessible to any user and will be deleted from that collection platform.

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.[8]

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 FISA-acquired information must receive training on these minimization procedures before

(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); and

(6) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States."

[7] [redacted]

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

~~SECRET//NOFORN~~

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.

~~(S//NF)~~ 2. [redacted] Nothing in these Procedures permits the retention of information obtained through unauthorized acquisitions.

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.

~~SECRET//NOFORN~~

4. (~~S//NF~~) FBI personnel are prohibited from accessing or reviewing unminimized data acquired pursuant to a certification entitled "In the Matter of [redacted] for any operational or analytical purpose, including to locate, understand, or produce foreign intelligence information or evidence of a crime. FBI personnel will not transfer any unminimized data acquired from Designated Accounts pursuant to a certification entitled "In the Matter of [redacted] to any FBI system used to conduct intelligence analysis, [redacted]

5. (~~S//NF~~) Backup copies. The FBI may temporarily retain emergency backup information in FBI collection platforms provided that only system administrators or other technical personnel have access to such information.[9] 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 an FBI collection platform or provide NSA or CIA lost, destroyed, or inaccessible data acquired under a certification entitled "In the Matter of [redacted] the FBI shall apply these procedures, including the applicable retention time limits for collection platforms, to the transferred data. FISA-acquired information retained under this subsection shall be destroyed within one-hundred-and-twenty (120) days of the date of acquisition.

[9] [redacted]

~~SECRET//NOFORN~~

6. ~~(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 section III.A.2 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] 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.

(U) ~~(S//NF)~~ If the FBI determines that a record captured by FBI's UAM activities contains section 702-acquired information, 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 for such purpose, 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.

B. (U) Additional Provisions Regarding Access, Review, and Use of FISA-Acquired Information

1. ~~(S//NF)~~ Procedures Regarding Access to FISA-Acquired Information Retained in Electronic Form. All FBI personnel having access to information acquired pursuant to a certification entitled "In the Matter of [redacted] will be informed of and provided access to these minimization procedures. The FBI may grant access to FISA-acquired information to all authorized technical and compliance personnel who have a need to access such information to perform their job duties or assist in a lawful and authorized government function. The FBI shall maintain accurate records of all persons to whom it has granted access to FISA-acquired information and shall require training on these minimization procedures for those personnel granted access to such information.

~~SECRET//NOFORN~~

~~(S//NF)~~ Should the FBI modify existing access policies or develop new policies regarding access to FISA information acquired pursuant to a certification entitled "In the Matter of [redacted] the FBI shall provide any new policies or materially modified policies to the Court on a semiannual basis.

(U) 2. ~~(S//NF)~~ Queries. Queries of unminimized section 702-acquired information are governed by Querying Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Concerning the International Production, Distribution, or Financing of Certain Illicit Drugs 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.

IV. (U) DISSEMINATION AND DISCLOSURE

(U) The dissemination provisions in these procedures apply only to information that FBI has properly retained in accordance with these procedures for security assessments of its systems or for UAM purposes. Section 702-acquired information may only be disclosed or disseminated for the purposes of remediating possible FISA compliance incidents or protecting against security vulnerabilities or for UAM purposes. 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, under the limited circumstances described below.

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

(U) Section 702-acquired information may be disclosed or disseminated to remediate possible FISA compliance incidents or to protect against security vulnerabilities or for UAM purposes. If 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 is discovered by FBI personnel performing duties related to those purposes, the FBI may disseminate such information 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 and must either:

1. reasonably appear 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; (iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (iv) international production, distribution, or financing of illicit synthetic drugs, opioids, cocaine, or other drugs driving overdose deaths, or precursors of any aforementioned; or

2. reasonably appear 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) As noted above, section 702-acquired information may be disclosed or disseminated to remediate possible FISA compliance incidents or to protect against security vulnerabilities or for UAM purposes. If FISA-acquired information concerning a United States person that reasonably appears to be evidence of a crime but not foreign intelligence information is discovered by FBI personnel performing duties related to those purposes, the FBI may disseminate such information for a law enforcement purpose 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 IV.

C. (U) Disclosure to the NSA and CIA.

(U) ~~(S//NF)~~ With respect to any FISA-acquired information from an electronic communication service provider, the FBI may convey such information to the NSA and CIA in unminimized form. The FBI may not convey such information to the National Counterterrorism Center (NCTC). The NSA and CIA shall handle any such unminimized information 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.

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. 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.

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 NSD.

12/11/24
Date

MATTHEW G. OLSEN
Assistant Attorney General for National Security