~~TOP SECRET//SI//NOFORN~~

(U) **EXHIBIT B**

(U) ~~(S//NF)~~ **MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY 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**

(U) Section 1 - Applicability and Scope

(U) These National Security Agency (NSA) minimization procedures apply to the acquisition, retention, use, and dissemination of information, including non-publicly 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 in accordance with section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA or "the Act"). 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.

(U) If NSA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) and that it is not feasible to obtain a timely modification of these procedures, NSA may take such action immediately. NSA will report the action taken to the Office of the Director of National Intelligence (ODNI) and to the National Security Division of the Department of Justice (NSD), which will promptly notify the Foreign Intelligence Surveillance Court (FISC) of such activity.

(U) For the purposes of these procedures, the terms "National Security Agency" and "NSA personnel" refer to any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to section 702 of the Act if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA).

(U) Section 2 - Exceptions, Oversight, and Training

(a) (U) NSA will conduct oversight (to include compliance) activities on an ongoing basis, with respect to its exercise of the authority under section 702 of the Act, including the targeting, minimization, and querying procedures adopted in accordance with section 702. NSA will develop and deliver training regarding the applicable procedures to ensure NSA personnel responsible for approving the targeting of persons for acquisition under section 702, as well as NSA personnel with access to information thereby acquired,

FILED UNDER SEAL

~~Classified by: The Attorney General~~
~~Derived From: NSA/CSSM 1-52 (dated 20180110)~~
~~Declassify On: 20500321~~

understand their responsibilities and the applicable procedures that apply to this acquisition. NSA will make any necessary reports, including those relating to incidents of noncompliance, to the NSA Inspector General and NSA Office of General Counsel, in accordance with its NSA charter. NSA will also ensure that necessary corrective actions are taken to address any identified deficiencies.

(b) (U) Nothing in these procedures shall restrict:

(1) (U) the performance of lawful oversight functions of NSD or ODNI, or the applicable Offices of the Inspectors General, or the provision by NSA of the assistance necessary for these entities to perform their lawful oversight functions;

(2) (U) activities necessary to create, test, or conduct technical maintenance of NSA systems that process or store section 702-acquired information;

(3) (U) 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 similar process consistent with congressional oversight;

(4) (U) NSA's ability to conduct vulnerability or network assessments using information acquired pursuant to section 702 in order to ensure that NSA systems are not or have not been compromised. Notwithstanding any other section in these procedures, information used by NSA to conduct vulnerability or network assessments may be retained for one year solely for that limited purpose. Any information retained for this purpose may be disseminated only in accordance with the applicable provisions of these procedures;

(5) (U) activities necessary to perform the following lawful oversight functions of NSA's personnel or systems:

a. (U) investigate and remediate possible section 702 compliance incidents;
b. (U) identify section 702-acquired information subject to destruction, including under these minimization procedures; or
c. (U) review, approve, or audit queries of section 702-acquired information.

(U) Should NSA determine it is necessary to deviate from an aspect of these procedures to perform lawful oversight functions of its personnel or systems apart from those described in this subsection (2.b.5), NSA shall consult with NSD and ODNI prior to conducting such an 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.

(c) (U) NSA has established internal procedures for ensuring that raw traffic is labeled and stored only in authorized repositories, and is accessible only to those who have had the proper training. NSA personnel who are undergoing, but have not yet completed, training regarding the proper implementation of section 702 and NSA's section 702 procedures may have access to raw section 702-acquired information during the conduct of such training and insofar as reasonably necessary to be effective.

(U) Whenever relying on any portion of the exceptions in this or the preceding subsection (2.b or 2.c) to deviate from any other provision of these minimization procedures, NSA personnel shall limit the scope of their deviation and comport with all other provisions of these minimization procedures to the maximum extent practicable.

(U) Section 3 - Definitions

(U) In addition to the definitions in sections 101 and 701 of the Act, the following definitions will apply to these procedures:

(a) (~~S//NF~~) Acquisition means the collection by NSA or the Federal Bureau of Investigation (FBI) through electronic means of a non-public communication to which it is not an intended party [redacted]

(b) (U) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly available information about the person.

(c) (U) Communications of a United States person include all communications to which a United States person is a party.

(d) (U) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken. Consent by an organization will be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement.

(e) (U) Foreign communication means a communication that has at least one communicant outside of the United States. All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications.

(f) (U) Identification of a United States person means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person.

~~TOP SECRET//SI//NOFORN~~

(g) ~~(TS//SI//NF)~~ Internet transaction, for purposes of these procedures, means an Internet communication that is acquired through NSA's upstream collection techniques. An Internet transaction may contain information or data representing either a discrete communication (e.g., an e-mail message) or multiple discrete communications [redacted]

(h) (U) Process or processing means any action necessary to convert unminimized section 702-acquired information into an intelligible form or any machine-initiated action designed to identify, curate, label, or organize such information; provided, however, that the term "process" or "processing" does not include an action that: (1) presents information for human inspection; or (2) using means that do not involve human inspection, produces and makes affirmative use of information for investigative, intelligence analysis, or preventative purposes.

(i) (U) Publicly available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation.

(j) (U) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person:

(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 NSA 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 NSA Office of General Counsel and NSD. 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 NSA 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.

(U) Section 4 - Acquisition and Handling - General

(a) (U) Acquisition

(U) The acquisition of information by targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Act will be effected in accordance with an authorization made by the Attorney General and Director of National Intelligence pursuant to subsection 702(a) of the Act and will be conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition.

(b) (U) Monitoring, Recording, and Handling

(1) (U) Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy information of or concerning a United States person at the earliest practicable point at which such information can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated under these procedures. Except as provided for in Section 4(c) below, such information of or concerning a United States person may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event.

(2) (U) Information of or concerning United States persons that may be related to the authorized purpose of the acquisition may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such information may be retained and disseminated only in accordance with Sections 4, 5, 6, 7, 8, and 11 of these procedures.

(3) (U) For purposes of assessing how information should be handled in accordance with these procedures, as information is reviewed, NSA analyst(s) will a) determine whether it is a domestic or foreign communication; b) ensure that it is not a communication that contains a reference to, but is not to or from, a target; and c) determine whether it is reasonably believed to contain foreign intelligence information or evidence of a crime.

(4) (U) Queries of unminimized content or noncontent 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. All such queries conducted by NSA personnel must be made in accordance with those procedures. Authorized NSA users with access to unminimized section 702-acquired

information should handle the results of an appropriate query of unminimized section 702-acquired information in accordance with these minimization procedures.

(U) Further handling, retention, and dissemination of foreign communications will be made in accordance with Sections 4, 5, 7, 8, and 11, as applicable, below. Further handling, storage, and dissemination of inadvertently acquired domestic communications will be made in accordance with Sections 4, 5, 6, and 8 below.

(c) (U) Destruction of Raw Data

(U) (1) ~~(TS//SI//NF)~~ Information acquired through tasking Internet selectors by or with the assistance of the FBI from Internet Service Providers or through tasking telephony selectors that does not meet the retention standards set forth in these procedures and that is known to contain information of or concerning United States persons will be destroyed upon recognition. Information acquired through tasking Internet selectors by or with the assistance of the FBI from Internet Service Providers or through tasking telephony selectors may not be retained longer than five years from the expiration date of the certification authorizing the collection unless NSA specifically determines that each specific item of acquired information meets the retention standards in these procedures.

(2) (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.[1]

(3) (U) In addition, NSA will follow the following procedures:

a. (U) Notwithstanding the destruction requirements set forth in these minimization procedures, NSA may retain specific section 702-acquired information if the Department of Justice advises NSA in writing that such information is subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation. The Department of Justice will identify in writing the specific information to be retained (including, but not limited to, the target(s) or selector(s) whose information must be preserved and the relevant time period at issue in the litigation), and the particular litigation for which the information will be retained. In order to restrict access to information being retained pursuant to this provision, personnel not working on the particular litigation matter shall not access the section 702-acquired information preserved pursuant to a written preservation notice from the Department of Justice that would otherwise have been destroyed pursuant to these procedures. Other personnel shall only access the information being retained for litigation-related reasons on a case-by-case basis after consultation with the Department of Justice. The Department of Justice shall notify NSA in writing once the section 702-acquired information is no longer

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

required to be preserved for such litigation matters, and then NSA shall promptly destroy the section 702-acquired information as otherwise required by these procedures.

1. (U) Each year, NSA and NSD will prepare a summary of: (a) all administrative, civil, or criminal litigation matters necessitating preservation of section 702-acquired data that would otherwise be subject to age off pursuant to these procedures, (b) a description of the section 702-acquired information preserved for each such litigation matter, and (c) if possible based on the information available to NSA, a description of the status of each such litigation matter.

2. (U) In certain circumstances, NSA may receive written notice from the Department of Justice advising NSA to preserve section 702-acquired information that would otherwise be subject to a destruction requirement under Sections 4(b)(1), 4(d)(2), 4(e), 5, or 6. NSA will promptly provide NSD with a summary of: (a) all administrative, civil, or criminal litigation matters necessitating preservation of section 702-acquired information that would otherwise be subject to destruction pursuant to Sections 4(b)(1), 4(d)(2), 4(e), 5, or 6, (b) a description of the section 702-acquired information preserved for each such litigation matter, and (c) if possible based on the information available to NSA, a description of the status of each such litigation matter. When such circumstances arise, NSD will promptly notify the FISC.

b. (U) The Department of Justice may advise NSA to retain specific section 702-acquired information subject to a destruction requirement other than those specified above in this section because such information is subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation. NSA will provide NSD with a summary of: (a) all administrative, civil, or criminal litigation matters necessitating preservation of section 702-acquired information that would otherwise be subject to destruction, (b) a description of the section 702-acquired information preserved for each such litigation matter, and (c) if possible, based on the information available to NSA, a description of the status of each such litigation matter. NSD will promptly notify and subsequently seek authorization from the FISC to retain the material as appropriate and consistent with law. NSA will restrict access to and retain such information in the manner described in Section 4(c)(4)(a), at the direction of the Department of Justice until either the FISC denies a government request for authorization to retain the information or the Department of Justice notifies NSA in writing that the information is no longer required to be preserved for such litigation matters. After receiving such notice, NSA shall promptly destroy the section 702-acquired information.

(d) (U) Change in Target's Location or Status

(1) (U) In the event that NSA reasonably believes that a target is located outside the United States and subsequently learns that the person is inside the United States, or if NSA concludes that a target who at the time of targeting was believed to be a non-United States person is in fact a United States person at the time of acquisition, the acquisition from that person will be terminated without delay.

(2) (U) Any information acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such information was acquired, and any information acquired by targeting a person who at the time of targeting was believed to be a non-United States person but was in fact a United States person at the time such information was acquired, will be treated as domestic communications under these procedures.

(e) ~~(S//NF)~~ In the event that NSA seeks to use any information acquired pursuant to section 702 during a time period when there is uncertainty about the location of the target of the acquisition because the [redacted] post-tasking checks described in NSA's section 702 targeting procedures were not functioning properly, NSA 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, NSA may not use or disclose any information acquired pursuant to section 702 during such time period unless NSA 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 NSA 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.

(f) (U) Additional Measures Regarding the Handling and Disposition of Improper Taskings

(U) (1) ~~(U//FOUO)~~ NSD shall promptly review the documentation from NSA of the basis for tasking selectors to section 702 acquisition. NSA shall cooperate in that effort. In the event such review leads NSD to assess that the basis for tasking any selector may be insufficient for targeting under a certification or authorization approved under section 702, or otherwise may not be in accordance with NSA's section 702 targeting procedures at the time of tasking, NSD will promptly provide NSA and ODNI with written notification of that assessment.

(U) (2) ~~(U//FOUO)~~ Upon receipt of such assessment by NSD, NSA shall promptly, and not later than 10 business days, initiate the steps required to (1) identify all information acquired from the tasking of that selector and reporting of such information and (2) place the identifiers for that information on the Master Purge List (MPL) or successor system as they are identified to limit further use or dissemination of that information. NSA shall promptly, and not later than 90 calendar days after written notification,

complete the steps required to identify and limit the use of all information acquired from the tasking. In the event that NSA is unable to complete these activities within the time periods specified in this paragraph, NSA will promptly report the reasons it is unable to do so to NSD and ODNI, and NSD will promptly notify the FISC in writing.

(U) (3) ~~(U//FOUO)~~ Once written notification has been made under Section 4(f)(1), NSD and ODNI shall make a final determination regarding the propriety of the tasking as expeditiously as practical. NSA shall cooperate in that effort. NSD shall promptly submit a written report to the FISC describing the circumstances for which a final determination has not been made within 60 calendar days of the written notification under Section 4(f)(1).

(U) (4) ~~(U//FOUO)~~ Upon written notification of a final determination by NSD and ODNI that the tasking of such selector was not proper under section 702 at the time of tasking, and following the completion of the steps required to identify and limit the use of all information acquired from the tasking as described in Section 4(f)(2), NSA shall promptly, and not later than 30 calendar days, complete the steps required for destroying all information acquired from the tasking of such selector and revise or recall relevant disseminations containing that information, informing the recipients of any recalled dissemination that it has been recalled as a result of a FISA-related compliance incident and therefore may not be further disclosed or used for any purpose. In the event that NSA is unable to complete these activities within 30 calendar days, NSA will promptly report the reasons it is unable to do so to NSD and ODNI, and NSD will promptly notify the FISC in writing.

(U) (5) ~~(U//FOUO)~~ Upon written notification of a final determination by NSD and ODNI that the tasking of a selector was proper, the identifiers for all such information identified through the steps described in Section 4(f)(2) may be removed from the MPL and such information will otherwise be handled in accordance with these procedures.

(U) Section 5 - Acquisition and Handling - Attorney-Client Communications

(U) Attorney-Client Privileged Communications. NSA may receive unminimized communications, acquired pursuant to section 702 of the Act, to which an attorney is a party. These provisions address the retention, dissemination, and use of information in such communications and apply when NSA personnel handling a communication acquired pursuant to section 702 of the Act determine (based on the information in that communication or other information of which the NSA personnel are aware) that the communication is between an attorney (or any person who, based on the information in the communication, appears clearly to be communicating on behalf of an attorney, such as an expert witness retained by the defense team, a paralegal, or administrative assistant) and a client.

~~TOP SECRET//SI//NOFORN~~

(a) (U) After discovering such a communication, if NSA personnel handling a communication make an affirmative determination that the communication does not contain foreign intelligence information or evidence of a crime, the communication must be destroyed irrespective of whether the communication contains information protected by the attorney-client privilege.

(b) (U) If NSA personnel handling such a communication determine that the communication appears to contain foreign intelligence information or evidence of a crime, the personnel handling the communication must bring the communication to the attention of NSA's Office of General Counsel for action as set forth below.

(c) ~~(S//NF)~~ Attorney-Client Privileged Communications Pertaining to a Criminal Charge in the United States. If the Office of General Counsel determines [redacted] If the communication contains attorney-client privileged information pertaining to a criminal charge in the United States, the communication shall be segregated.

(d) [redacted]

(e) ~~(S//NF)~~ [redacted] If the communication contains attorney-client privileged information, the communication shall be segregated.

(f) [redacted] he

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

(g) ~~(S//NF)~~ [redacted] dissemination of attorney-client privileged information of the type described in subparagraphs (c) and (e) above outside NSA shall be limited [redacted] accompanied by appropriate handling controls, and shall include language advising recipients (1) that the report contains information obtained from communications that may be subject to the attorney-client privilege, (2) that use of the information is provided for intelligence purposes only and may not be used in any trial, hearing, or other proceeding absent express approval by the Attorney General, and (3) that further dissemination is prohibited absent the express approval of the Assistant Attorney General for National Security [redacted]

(h) [redacted]

(i) [redacted]

(U) Section 6 - Domestic Communications

(U) A communication identified as a domestic communication (and, if applicable, the Internet transaction in which it is contained), including information treated as a domestic communication, will be promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing and on a communication-by-communication basis, that the sender or intended recipient of the domestic communication had been properly targeted under section 702 of the Act, and the domestic communication satisfies one or more of the following conditions:

(1) (U) such domestic communication is reasonably believed to contain significant foreign intelligence information. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained, handled, and disseminated in accordance with these procedures;

(2) (U) such domestic communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such domestic communication may be disseminated in accordance with Section 8(b)(9) below. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained by NSA for a reasonable period of time, not to exceed six months unless extended in writing by the Attorney General, to permit law enforcement agencies to determine whether access to original recordings of such communication is required for law enforcement purposes;

(3) (U) such domestic communication is necessary to understand or assess a communications security vulnerability of a United States Government or National Security system. Such domestic communication may be provided to the FBI and/or disseminated to other elements of the United States Government. Such domestic communication (and, if applicable, the transaction in which it is contained) may be retained for a period of time during which such information is of use in identifying or defending against such a vulnerability; or

(4) (U) such domestic communication contains information pertaining to an imminent threat of serious harm to life or property. Such information may be retained and disseminated to the extent reasonably necessary to counter such threat.

(U) Notwithstanding the above, if a domestic communication indicates that a target has entered the United States, NSA may promptly notify the FBI of that fact, as well as any information concerning the target's location that is contained in the communication. NSA may also use information derived from domestic communications for collection avoidance purposes, and may provide such information to the FBI, Central Intelligence Agency (CIA), and National Counterterrorism Center (NCTC) for purposes of collection avoidance. NSA may retain the communication from which such information is derived but shall restrict the further use or dissemination of the communication by placing it on the MPL.

(U) NSA will report all determinations made by the Director (or the Acting Director) of NSA under this Section to ODNI and NSD, which will promptly notify the FISC in writing of all such determinations.

(U) Section 7 - Retention of Foreign Communications of or Concerning United States Persons

(U) Foreign communications of or concerning United States persons collected in the course of an acquisition authorized under section 702 of the Act may be retained as follows:

(1) (U) Retention of foreign communications of or concerning United States persons is permitted for a period of five years from the expiration date of the certification authorizing the collection, unless the Director, Operations Directorate, NSA, determines in writing that retention of a specific category of communications for a longer specified period is required to respond to authorized foreign intelligence or

counterintelligence requirements. NSA will report all such determinations to ODNI and NSD, which will promptly notify the FISC in writing of all such determinations.

a. (U) NSA may also retain unminimized section 702-acquired information that reasonably appears to be encrypted or to contain secret meaning for a sufficient duration to permit exploitation. A sufficient duration may consist of any period of time during which the encrypted information is subject to, or of use in, cryptanalysis or deciphering secret meaning. Once information is decrypted or deciphered, the retention period, if applicable for such information, is five years from the date of decryption or decipher.

(2) (U) if dissemination of such communications with reference to such United States persons would be permitted under Section 8 below; or

(3) (U) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities, consistent with the dissemination provisions below.

(U) Nothing in this section shall preclude NSA from retaining technical information (e.g. encryption algorithms, keys, credentials) contained in, or derived from, foreign communications of or concerning United States persons for any period of time during which such information is used for cryptanalysis or processing information into intelligible form. Any use or dissemination of such technical information must be made in accordance with the requirements in these procedures.

(U) Section 8 - Dissemination

(a) (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.

(1) (U) In making determinations regarding whether non-publicly available information that identifies any United States person constitutes foreign intelligence information as defined in 50 U.S.C. § 1801(e), NSA personnel must bear in mind that FISA's definition of foreign intelligence information in 50 U.S.C. § 1801(e) requires that information concerning a United States person must be "necessary to" the ability of the United States to protect against certain threats identified in 50 U.S.C. § 1801(e)(1) or be "necessary to" the national defense or the security of the United States or the conduct of the foreign affairs of the United States, as specified in 50 U.S.C. § 1801(e)(2).

(2) (U) In order to be "necessary to" these topics, non-publicly available information identifying a United States person must be more than merely useful or convenient.

Instead, there must be a significant need for the information about a United States person to enable the United States to protect against one or more of the threats specified in 50 U.S.C. § 1801(e)(1) or to support the national defense or security of the United States or the conduct of the foreign affairs of the United States, as specified in 50 U.S.C. § 1801(e)(2). In making this assessment, consideration should be given to demonstrating the nexus between the United States person information to be disseminated and the threats identified in 50 U.S.C. § 1801(e)(1) or, as discussed in 50 U.S.C. § 1801(e)(2), the national defense, the security of the United States, or the conduct of the foreign affairs of the United States. However, the information need not be the only means of accomplishing these goals and the necessity of the information can be considered in the context of other information available to the United States.

(3) (U) With respect to foreign intelligence information as defined in 50 U.S.C. § 1801(e)(1)(D), in particular—i.e., information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against the international production, distribution, or financing of illicit synthetic drugs, opioids, cocaine, or other drugs driving overdose deaths, or precursors of any aforementioned (collectively "international drug trafficking")—NSA personnel must ensure that the non-publicly available information that identifies a United States person is important and required to enable the United States to protect against this identified threat before determining that it constitutes foreign intelligence information. This determination must be particularized and fact-based, informed by analytic judgment and the specialized training and experience of the analyst.

a. ~~(S//NF)~~ NSA personnel may encounter a variety of types of information acquired pursuant to a certification entitled "In the Matter of [redacted]. Such information could include information that is necessary to the United States' ability to protect against international drug trafficking, but it also could include information that merely relates to this ability, information that concerns illicit drug production, distribution, or financing with no international nexus, or information that is unrelated to illicit drugs at all.[2] Of these categories, with respect to United States persons, only information that is necessary to protect against international drug trafficking qualifies as foreign intelligence information as defined in 50 U.S.C. § 1801(e)(1)(D).

(b) (U) A dissemination based on information of or concerning a United States person may be made if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise, dissemination of intelligence based on information of or concerning a United States person may only be made to a recipient

(U)

[2] ~~(S//NF)~~ For example, NSA personnel could encounter information regarding the licit production, distribution, or financing of opioids. This would necessarily not be either foreign intelligence information or evidence of a crime.

requiring the identity of such person for the performance of official duties but only if (i) an affirmative determination is made regarding the necessity to include the identity of the United States person, (ii) at least one of the following criteria is also met, and (iii) the basis for both of the foregoing determinations is documented:

(1) (U) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;

(2) (U) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;

(3) (U) the information indicates that the United States person may be:

a. an agent of a foreign power;

b. a foreign power as defined in section 101(a) of the Act;

c. residing outside the United States and holding an official position in the government or military forces of a foreign power;

d. a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

e. acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material;

(4) (U) the information indicates that the United States person may be the target of intelligence activities of a foreign power;

(5) (U) the information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information, but only after the agency that originated the information certifies that it is properly classified;

(6) (U) the United States person's identity is necessary to understand or assess a communications or network security vulnerability;

(7) (U) the information indicates that the United States person may be engaging in international terrorist activities;

(8) (U) the acquisition of the United States person's information was authorized by a court order issued pursuant to the Act and the information may relate to the foreign intelligence purpose of the surveillance; or

~~TOP SECRET//SI//NOFORN~~

(9) (U) the identity of the United States person is not necessary to understand foreign intelligence information or assess its importance, but the information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, and provided that dissemination is to the FBI or other appropriate federal law enforcement authorities for law enforcement purposes, as follows:

a. ~~(S//NF)~~ to the extent information of or concerning a United States person solely is being disseminated because it is reasonably believed to contain evidence that a violation of U.S. drug laws has been, is being, or is about to be committed, such information may be disseminated only [redacted] determines in writing that the dissemination satisfies one or more of the following conditions:

(U) 1. ~~(S//NF)~~ the dissemination is made in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document, and the information is reasonably believed to contain evidence of a violation of United States criminal law involving either significant quantities of illicit drugs or activities that increase the lethality of illicit drugs, and is necessary to protect against serious crime;

2. (U) the information is necessary to understand or assess a communications security vulnerability of a United States Government or National Security system. Such information may be provided to the FBI and/or disseminated to other elements of the United States Government; or

3. (U) the information pertains to an imminent threat of serious harm to life or property. Such information may be disseminated to the extent reasonably necessary to counter such threat.

b. (U) the information concerns possible evidence of any other crime and is made in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document.

(10) ~~(S//NF)~~ To the extent information of or concerning a United States person is retrieved in response to a query conducted in support of vetting non-United States persons pursuant to subsection IV.D.3 of the NSA Section 702 Querying Procedures, such information may only be disseminated [redacted]

[redacted] determines in writing that the dissemination satisfies one or more of the following conditions:

a. (U) such information is reasonably believed to contain significant foreign intelligence information and is necessary to protect against international terrorism or any threat described in 50 U.S.C. § 1801(e)(1)(D);

b. (U) such information does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed, and is disseminated consistent with subsection 8(b)(9) of these procedures;

c. (U) such information is necessary to understand or assess a communications security vulnerability of a United States Government or National Security system. Such information may be provided to the FBI and/or disseminated to other elements of the United States Government; or

d. (U) the information pertains to an imminent threat of serious harm to life or property. Such information may be disseminated to the extent reasonably necessary to counter such threat.

(U) Section 9 - Provision of Unminimized Information to CIA

(U) NSA may provide to CIA unminimized information acquired pursuant to section 702 of the Act. CIA will identify to NSA targets for which NSA may provide unminimized information to CIA. CIA will handle any such unminimized information received from NSA in accordance with CIA minimization and querying procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsections 702(e) and 702(f) of the Act, respectively.

~~(S//NF)~~ ~~(U)~~ NSA may not provide to the FBI or NCTC unminimized information acquired pursuant to any section 702 certification entitled "In the Matter of [redacted]

(U) Section 10 - Other Foreign Communications

(U) Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy.

~~TOP SECRET//SI//NOFORN~~

(U) Section 11 - Collaboration with Foreign Governments

(a) (U) Procedures for the dissemination of evaluated and minimized information. Pursuant to section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may be disseminated to a foreign government. Except as provided below in Section 11(b) of these procedures, any dissemination to a foreign government of information of or concerning a United States person that is acquired pursuant to section 702 may only be done in a manner consistent with Section 8 of these NSA minimization procedures.

(b) (U) Procedures for technical or linguistic assistance. It is anticipated that NSA may obtain information that, because of the information's technical or linguistic content, may require further analysis by foreign governments to assist NSA in determining the information's meaning or significance. Notwithstanding other provisions of these minimization procedures, NSA may disclose computer disks, tape recordings, transcripts, or other information or items containing unminimized information acquired pursuant to section 702 to foreign governments for further processing and analysis, under the following restrictions with respect to any materials so disclosed:

(1) (U) Disclosure to foreign governments will be solely for translation or analysis of such information, and assisting foreign governments will make no use of any information of or concerning any person except to provide technical and linguistic assistance to NSA.

(2) (U) Disclosure will be only to those personnel within foreign governments involved in the translation or analysis of such information. The number of such personnel will be restricted to the extent feasible. There will be no disclosure within foreign governments of this unminimized data.

(3) (U) Foreign governments will make no permanent agency record of information of or concerning any person referred to or recorded on computer disks, tape recordings, transcripts, or other items disclosed by NSA to foreign governments, provided that foreign governments may maintain such temporary records as are necessary to enable them to assist NSA with the translation or analysis of such information. Records maintained by foreign governments for this purpose may not be disclosed within the foreign governments, except to personnel involved in providing technical or linguistic assistance to NSA.

(4) (U) Upon the conclusion of such technical or linguistic assistance to NSA, computer disks, tape recordings, transcripts, or other items or information disclosed to foreign governments will either be returned to NSA or be destroyed with an accounting of such destruction made to NSA.

~~TOP SECRET//SI//NOFORN~~

(U) Any information that foreign governments provide to NSA as a result of such technical or linguistic assistance may be disseminated by NSA in accordance with these minimization procedures.

(U) Section 12 - NSA User Activity Monitoring

(~~S//NF~~) As required by numerous statutes and regulatory issuances, NSA conducts user activity monitoring of its internal computer systems and networks to deter, detect, and otherwise protect against unauthorized access or use of those systems and networks, and classified or other sensitive data that is stored, processed, or transmitted on those systems and networks. These security activities include [redacted] user activity monitoring activities may be retained indefinitely in NSA user activity monitoring systems and used by NSA solely to deter, detect, and otherwise protect against unauthorized access and use of NSA's systems and networks. Access to any NSA user activity monitoring system that may contain unminimized section 702-acquired information shall be limited to NSA personnel who require access to perform their official duties related to user activity monitoring. [redacted] Any personnel with access to such systems must receive training on these procedures. NSA shall maintain records of all personnel who have access to user activity monitoring systems. In the event NSA recognizes a record that contains unminimized section 702-acquired information in an NSA user activity monitoring system, any dissemination of section 702-acquired information must be made in accordance with the dissemination requirements in these procedures.

3/19/25
Date

PAMELA BONDI
Attorney General of the United States

~~TOP SECRET//SI//NOFORN~~