DoD Manual S-5240.01-A

(U) Procedures Governing the Conduct of DoD Intelligence Activities: Annex Governing Signals Intelligence Information and Data Collected Pursuant to Section 1.7(c) of E.O. 12333

Originating Component:	Office of the Chief Management Officer of the Department of Defense
Effective:	January 7, 2021
Releasability:	Not cleared for public release. Contact the Office of the Chief Management Officer for a copy.
Supersedes and Repeals:	See Reference Group
Approved by:	William P. Barr, Attorney General of the United States Mark T. Esper, Secretary of Defense

Purpose: (U) DoD Manual (DoDM) 5240.01, including this annex, establishes procedures to conduct authorized activities in a manner that protects the constitutional and other legal rights of U.S. persons and persons in the United States as well as the privacy and civil liberties of such persons. This annex:

- (U) Implements Section 2.3 of Executive Order (E.O.) 12333 and provides additional governance for the collection, processing, querying, retention, and dissemination of signals intelligence (SIGINT) information and data collected by the United States SIGINT System (USSS).
- (U) Governs how the USSS will fulfill its existing responsibilities and does not confer any new authorities.

(U) Table of Contents

SECTION 1: (U) GENERAL ISSUANCE INFORMATION

1.1. (U) INTRODUCTION.

a. (U) Section 1.10(e) of E.O. 12333, as amended, provides that the Secretary of Defense acts, in coordination with the Director of National Intelligence (DNI), as the executive agent of the U.S. Government for SIGINT activities. In Section 1.7(c), the Director of the National Security Agency/Chief of the Central Security Service (DIRNSA/CHCSS), referred to in this annex as the DIRNSA, is authorized to collect (including through clandestine means), process, analyze, produce, and disseminate SIGINT information and data for foreign intelligence and counterintelligence purposes, and to provide SIGINT support for national and departmental requirements and for the conduct of military operations.

b. (U) The DIRNSA serves as the Intelligence Community's Functional Manager for SIGINT in accordance with E.O. 12333 and is directed to control SIGINT collection and processing activities. E.O. 12333 requires the DIRNSA to establish and operate an effective, unified organization for SIGINT activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community.

c. (U) Except as specifically provided in this annex, all activities undertaken in accordance with this annex must also comply with the procedures promulgated by the Secretary of Defense and approved by the Attorney General in DoDM 5240.01.

1.2. (U) APPLICABILITY.

a. (U) This annex applies to the USSS and regulates SIGINT activities conducted under the DIRNSA's SIGINT authority. SIGINT includes, individually or in combination, communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). This annex governs the collection, processing, querying, retention, and dissemination of all COMINT by the USSS. It also governs any ELINT, FISINT, non-communications and non-communications related data, telemetry, radar emissions, or direction-finding activities conducted by the USSS that implicate the Fourth Amendment to the Constitution. References to "SIGINT," "communications," or "information" in this annex apply to all forms of communications, non-communications, and data regulated by this annex unless otherwise specified in this annex (e.g., references to communications metadata).

b. (U) Appendix 7A pertains to collection activities that target U.S. persons outside the United States under Section 2.5 of E.O. 12333 and Sections 704, 705(b), or 705(c) of the Foreign Intelligence Surveillance Act (FISA) (Sections 1881c-d of Title 50, United States Code (U.S.C.)). Except as indicated in Appendix 7A, this annex does not govern activities by the USSS that are conducted pursuant to FISA.

c. (U) This annex does not apply to dissemination by the National Security Agency (NSA) of unevaluated SIGINT to other elements of the Intelligence Community as directed by the President or as permitted under other procedures approved by the Attorney General, including

the "Procedures for the Availability or Dissemination of Raw Signals Intelligence Information by the National Security Agency under Section 2.3 of Executive Order 12333 (Raw SIGINT Availability Procedures)."

1.3. (U) GENERAL PROVISIONS.

a. (U) U.S. Person Presumptions.

(U) The following guidelines apply when determining whether an individual or entity is a U.S. person:

(1) (U) A person or organization in the United States is presumed to be a U.S. person, unless specific information to the contrary is obtained.

(2) (U) A person or organization outside the United States, or whose location is not known to be in the United States, is presumed to be a non-U.S. person, unless specific information to the contrary is obtained.

b. (U) Activities by Foreign Cryptologic Partners.

(U) SIGINT collection and other SIGINT activities conducted with foreign cryptologic partners must meet the requirements of this annex. Providing technical equipment, funds, or other assistance to such partners for the purpose of SIGINT collection directed at a particular U.S. person must be treated under this annex as if undertaken directly by the USSS.

c. (U) Internal Guidance.

(U) This annex is published solely for the purpose of internal USSS guidance. It is not intended to, does not, and may not be relied on to create any rights, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person, nor does it place any limitation on otherwise lawful investigative and litigative prerogatives of the United States.

d. (U) Delegation, Interpretation, Exceptions, and Amendments.

(U) The USSS will refer questions about the applicability or interpretation of this annex to NSA's Office of General Counsel (OGC). The USSS will follow Procedure 1 of DoDM 5240.01 to determine who may approve particular activities or take particular actions; how this annex is to be interpreted, including when referrals to the Department of Justice and the Office of the Director of National Intelligence (ODNI) should be made; and when exceptions or amendments to this annex are needed. Notwithstanding the foregoing, the DIRNSA and the Attorney General, after consulting with DoD OGC and ODNI, may approve exceptions or amendments to Appendix 7A.

e. (U) Attorney-Client Communications.

(U) The USSS must comply with guidance promulgated by the Attorney General with respect to the processing, querying, retention, and dissemination of attorney-client communications. The Attorney General will consult with the General Counsel of the Department of Defense before promulgating such guidance.

f. (U) Limited Exceptions to the Processing, Querying, Retention, and Dissemination Rules.

(1) (U) Due Diligence Activities.

(U) Subject to section 6, and notwithstanding any other restrictions in this annex, the USSS may engage in due diligence activities that are intended to avoid or remove unauthorized collection, reduce unwanted collection, promote adherence to restrictions against the deliberate retrieval of U.S. person information (USPI), ensure the effective application of retention restrictions, and aid the USSS in determining whether USPI must be minimized when disseminating communications. These due diligence activities include, but are not limited to:

(a) (U) Processing and querying information for the limited purpose of ascertaining whether a potential target is a U.S. person or is located in the United States. Such due diligence activities will be designed to limit to the greatest extent practicable the review of the contents of communications that contain USPI.

(b) (U) Retaining and disseminating information for collection avoidance purposes.

(2) (U) Data Backup.

(U) The USSS may process, query, retain, and disseminate information for data backup purposes. Access to this information will be limited to only those personnel responsible for maintaining and administering information systems and networks. In the event that information retained for data backup purposes must be used to restore lost, destroyed, or inaccessible information, the USSS must apply this annex to the restored information. Information will be retained for data backup purposes only for such time as is reasonably necessary for the purposes in this annex, including the purposes identified in this section.

(3) (U) Vulnerability Assessments.

(U) The USSS may process, query, retain, and disseminate information to conduct vulnerability or network assessments in order to ensure that USSS systems are not or have not been compromised. Notwithstanding any other section in this annex, information used by the USSS to conduct vulnerability or network assessments may be retained for 1 year solely for that limited purpose.

(4) (U) Court Orders and Congressional Requests.

(U) The USSS may process, query, retain, and disseminate information to comply with a litigation hold, preservation directive, or court order; a specific congressional request, after

consultation with the Attorney General; or a directive of the Attorney General. Any activity under this provision must be coordinated with NSA OGC. The USSS will limit access to the information being retained for litigation-related reasons on a case-by-case basis to only those individuals necessary.

(5) (U) Oversight Functions.

(U) The USSS may process, query, retain, and disseminate information necessary for the performance of lawful oversight functions, including lawful oversight functions of the Congress, the Department of Justice, DoD, ODNI, the Privacy and Civil Liberties Oversight Board, or the applicable offices of the Inspectors General.

1.4. (U) INFORMATION COLLECTIONS.

(U) Information collected during intelligence activities, referred to throughout this issuance, does not require licensing with a report control symbol in accordance with Paragraphs 1.b.(3) and 1.b.(8) of Enclosure 3 of Volume 1 of DoD Manual 8910.01, or licensing with an Office of Management and Budget Control Number in accordance with Paragraph 8.a.(2)(d) of Enclosure 3 of Volume 2 of DoD Manual 8910.01.

SECTION 2: (U) COLLECTION

2.1. (U) SCOPE.

(U) This section governs SIGINT collection by the USSS under E.O. 12333 to satisfy foreign intelligence or counterintelligence requirements, to provide support to military operations, or, as specified in Paragraph 2.5.c, to protect the safety or enable the recovery of a U.S. person captive.

2.2. (U) GENERAL.

a. (U) The USSS may collect SIGINT inside or outside the United States by any lawful means authorized under E.O. 12333, provided that the USSS may not intentionally target U.S. persons or persons in the United States unless authorization has been obtained in accordance with this section or FISA. The USSS:

(1) (U) Will limit SIGINT collection in accordance with Paragraph 3.2.f.(4) of DoDM 5240.01.

(2) (U) Will conduct targeted collection using selection terms whenever practicable, but may use other discriminants or conduct bulk collection when necessary due to technical or operational considerations.

(3) (U) Will take reasonable steps to determine the non-U.S.-person status and location of a current or potential target.

b. (U) It is possible that the USSS may incidentally collect domestic communications and communications to, from, or about U.S. persons in the course of authorized collection of foreign communications. The USSS will make every reasonable effort through surveys and technical means to reduce, to the maximum extent possible, the number of such incidentally collected communications. The USSS will handle such incidentally collected communications in accordance with this annex.

2.3. (U) COLLECTION CONSIDERATIONS.

a. (U) In conducting collection and in developing collection techniques, the USSS, consistent with mission requirements and internal policy, will consider all of the following factors:

(1) (U) Methods to limit the collection of USPI that is not responsive to the foreign intelligence, counterintelligence, or support to military operations purposes of the collection or, in the case of collection under Paragraph 2.5.c., the purpose of protecting the safety or enabling the recovery of the U.S. person captive.

(2) (U) Methods to limit the types and aspects of the information collected to those relevant to the purposes of the collection.

(3) (U) Whether mission requirements can be met by filtering non-pertinent information as soon as practicable after collection.

(4) (U) If any activity covered by this annex is deemed to constitute special circumstances collection as defined by Paragraph 3.2.e. of DoDM 5240.01.

b. (U) In accordance with Paragraph 2.3.a. the USSS will consider whether additional approvals or civil liberties and privacy protections are needed and, if so, identify the USSS entities responsible for implementing those requirements.

2.4. (U) PROHIBITIONS ON COLLECTION.

a. (U) Domestic Communications.

(U) The USSS will not intentionally collect domestic communications unless authorized in accordance with:

(1) (U) Paragraph 2.5;

(2) (U) Paragraph 3.5.i., 3.5.j., or 3.5.k. of DoDM 5240.01; or

(3) (U) FISA.

b. (U) Reverse Targeting.

(U) The USSS will not intentionally collect foreign communications for the purpose of targeting a specific U.S. person or person in the United States unless such U.S. person or person in the United States has been separately authorized for targeting under this annex or FISA.

2.5. (U) LIMITATIONS ON COLLECTION.

a. (U) Limitations on Certain Collection Methods.

(1) (U) SIGINT Collection Based on Selection Terms or Other Discriminants.

~~(S//SI//REL)~~ The USSS may collect SIGINT using selection terms, whether the terms identify a target, a subject matter or a characteristic of the communication, or a combination of these elements, or other discriminants. Selection terms or other discriminants that are reasonably likely to result in, or have resulted in, the collection of communications to, from, or about U.S. persons (wherever located) will be designed to defeat, as practicable under the circumstances, the collection of those communications, or data related to those communications, that do not contain foreign intelligence, counterintelligence, information in support of military operations, or, in the case of collection under Paragraph 2.5.c., information necessary to protect the safety or enable the recovery of the U.S. person captive.

EO 1.4.(c)
PL 86-36/50 USC 3605

(a) (U) SIGINT Over Radio Channels with a Terminal in the United States.

~~(S//SI//REL)~~ When collecting foreign radio communications [redacted] that pass over a channel with a terminal in the United States, the USSS will target non-U.S. persons outside the United States and use selection terms, except that the requirement to use selection terms does not apply if the communications take place over a channel used exclusively by a foreign power.

(b) ~~(S//SI//REL)~~ [redacted] Used by a Foreign Entity.

~~(S//SI//REL)~~ Communications [redacted] with a terminal in the United States that service a U.S. person may be collected using selection terms upon certification in writing by the DIRNSA or a delegee to the Attorney General.

1. (U) The certification must:

a. (U) Confirm that the target of the collection is a non-U.S. person outside the United States; that the collection technique does not fall within FISA's definition of electronic surveillance; and that the purpose of the collection is to obtain foreign intelligence or counterintelligence; and

b. (U) State the purpose of the collection; describe the entity or entities that may be targeted; affirm that legal, civil liberties, and privacy officials have been consulted; and describe the minimization procedures that will be applied.

2. (U) The certifying official will report on substantial changes to the collection as provided in Paragraph 6.6.b.

(2) (U) Surveys.

(a) (U) The USSS may conduct surveys only of the signals environment and only for the purposes of identifying those signals or communications that:

1. (U) May contain information related to the production of foreign intelligence or counterintelligence;

2. (U) Are enciphered or appear to contain secret meaning and are needed to develop technical capabilities;

3. (U) Are needed to ensure efficient SIGINT collection or to avoid the collection of unwanted signals; or

4. (U) Reveal U.S. communications security vulnerabilities.

(b) (U) Surveys must be reasonable and appropriately limited in scope, output, and duration.

(c) (U) Surveys must not be used as a substitute for sustained collection, and the USSS may not, as part of a survey, engage in electronic surveillance as defined by FISA, unless the survey is otherwise permitted by FISA and Procedure 5 of DoDM 5240.01. The USSS:

1. (U) May survey communications channels with a terminal in the United States only when necessary to determine whether a channel contains SIGINT information of foreign intelligence or counterintelligence interest for USSS collection. The DIRNSA or a delegee must approve any such collection without the use of selection terms if the collection will exceed 2 hours.

2. (U) Will, in any event, limit the collection to the minimum amount of time necessary to determine the nature of the SIGINT information on the channel and whether that information has intelligence value.

b. (U) Limitations on Collection Targeting U.S. Persons.

(U) The USSS may intentionally target a U.S. person, whether inside or outside the United States, only if the collection is not governed by FISA and one of the following circumstances exists:

(1) (U) Consent.

(U) With appropriate consent of the U.S. person, or a third party (i.e., an individual or organization) who is legally authorized to consent on behalf of the U.S. person, provided on a case-by-case basis.

(2) (U) Agent, Officer, or Employee of a Foreign Power.

(U) With the specific prior approval of the Attorney General for a period of time not to exceed 90 days if both of the following apply:

(a) (U) The Attorney General determines that there is probable cause to believe that the U.S. person is an agent of a foreign power or an officer or employee of a foreign power.

(b) (U) The purpose of the collection is to acquire significant foreign intelligence or counterintelligence.

(3) (U) Exigent Circumstances.

(U) If electronic surveillance of a U.S. person has been authorized in accordance with Paragraph 3.5.h. of DoDM 5240.01, which addresses exigent circumstances outside the United States.

c. (U) U.S. Person Captives.

(U) The USSS may provide SIGINT support for national and departmental requirements and for the conduct of military operations, as follows, when the collection is not governed by FISA

and is necessary to protect the safety or enable the recovery of a U.S. person held captive outside the United States:

(1) (U) Scope.

(U) When a U.S. person outside the United States is reasonably believed to be held captive by a foreign power or other non-U.S. person, the USSS may intentionally collect SIGINT information that is necessary to protect the safety or enable the recovery of that person.

(2) (U) Targeting of U.S. Persons.

(a) (U) Any intentional targeting of a U.S. person captive described in Paragraph 2.5.c.(1) must be for the purpose of supporting national or departmental requirements or the conduct of military operations concerning the safety or recovery of the U.S. person captive and limited to identifying:

1. (U) The captive's location;

2. (U) The captive's physical and mental condition;

3. (U) The degree of risk associated with conducting a recovery operation or facilitating the captive's escape;

4. (U) The identities and affiliations of the captors; or

5. (U) The vulnerabilities of the captors or captor network.

(b) (U) The intentional targeting of any U.S. person other than a U.S. person captive described in Paragraph 2.5.c.(1) is not authorized, except as otherwise permitted by this annex.

(3) (U) Targeting of Non-U.S. Persons.

(U) The intentional targeting of a non-U.S. person located in the United States is not authorized, except as otherwise permitted by this annex.

(4) (U) Approval.

(U) Collection under Paragraph 2.5.c.(2)(a) requires the specific, prior approval of the DIRNSA or a delegee and may be authorized for a period not to exceed 90 days.

(5) (U) Notification.

(U) NSA OGC will promptly notify the National Security Division of the Department of Justice when the DIRNSA or a delegee authorizes collection under Paragraph 2.5.c.(2)(a), or approves the continuation of previously authorized collection.

d. (U) Limitations on Collection Targeting Non-U.S. Persons in the United States.

(U) The USSS may intentionally target a non-U.S. person in the United States only if the collection is not governed by FISA and if one of the following circumstances exists:

(1) (U) Consent.

(U) With appropriate consent of the person, or a third party (i.e., an individual or organization) who is legally authorized to consent on behalf of the person, provided on a case-by-case basis.

(2) ~~(S//SI//REL)~~ [redacted]

~~(S//SI//REL)~~ The USSS may intentionally target a non-U.S. person in the United States [redacted] for the purpose of acquiring significant foreign intelligence or counterintelligence if all of the following apply:

(a) ~~(S//SI//REL)~~ The USSS confirms that the target is [redacted]

(b) (U) The DIRNSA or a delegee approves the collection.

(c) (U) The collection is limited to communications where at least one of the communicants is outside the United States at the time of acquisition. When it is not possible to limit collection in this manner, the Attorney General must approve the collection.

(3) ~~(S//SI//REL)~~ [redacted] Business Entity Controlled by a Foreign Government.

~~(S//SI//REL)~~ The USSS may intentionally target [redacted] foreign power, as that term is defined at Paragraphs (1) - (3) of the Glossary's definition of a "foreign power," or a business entity in the United States that is openly acknowledged to be directed and controlled by a foreign government or governments, for a period of up to one year with the specific prior approval of the Attorney General, if both of the following apply:

(a) (U) The Attorney General determines that there is probable cause to believe that the target is such an establishment or business entity.

(b) (U) The purpose of the collection is to acquire significant foreign intelligence or counterintelligence.

(4) (U) Agent of a Foreign Power.

(U) The USSS may intentionally target a non-U.S. person who is inside the United States for up to 90 days with the specific prior approval of the Attorney General if both of the following apply:

(a) (U) The Attorney General determines that there is probable cause to believe that the person is an agent of a foreign power.

(b) (U) The purpose of the collection is to acquire significant foreign intelligence or counterintelligence.

(5) (U) Target Entering the United States.

(a) (U) If the USSS is intentionally targeting a non-U.S. person who enters the United States, the USSS may continue collection of the communications for a period not to exceed 72 hours after it is learned that the non-U.S. person is in the United States if securing the prior approval of the Attorney General for continued collection is not practicable and all of the following apply:

1. (U) Circumstances suggest that the target is an agent of a foreign power.

2. (U) There are reasonable grounds to believe that a lapse in targeting would:

a. (U) Pose an imminent threat of (i) death or serious bodily harm to any person or (ii) destruction of, or significant damage to, property; or

b. (U) Cause a failure to obtain significant foreign intelligence or counterintelligence, or a delay in obtaining such information, that would result in substantial harm to national security.

3. (U) The DIRNSA or a delegee approves the collection.

(b) (U) The USSS must notify the Attorney General as soon as possible of any collection authorized under this provision, including the circumstances supporting its authorization.

(c) (U) Collection targeting the non-U.S. person under the authority of Paragraph 2.5.d.(5)(a) is limited to a period not to exceed 72 hours, and the USSS must cease collection pursuant to that authority before the end of that 72-hour period upon the earliest of the following:

1. (U) The USSS confirms that it already has authorization under other provisions of this annex to collect such communications;

2. (U) The USSS obtains authorization to conduct the collection in a manner prescribed by FISA or this annex by:

a. ~~(S//SI//REL)~~ Confirming that the person [redacted] and continuing the collection in accordance with Paragraph 2.5.d.(2);

b. (U) Obtaining a determination from the Attorney General that there is probable cause to believe that the person is an agent of a foreign power in accordance with Paragraph 2.5.d.(4); or

c. (U) Obtaining authorization from the Attorney General or the Foreign Intelligence Surveillance Court to collect the person's communications in accordance with FISA;

3. (U) The Attorney General directs that the intentional targeting of the non-U.S. person for collection under Paragraph 2.5.d.(5)(a) be terminated; or

4. (U) The exigency authorizing collection under Paragraph 2.5.d.(5)(a) no longer exists because there are no longer reasonable grounds to believe that a lapse in targeting would:

a. (U) Pose an imminent threat of (i) death or serious bodily harm to any person or (ii) destruction of, or significant damage to, property; or

b. (U) Cause a failure to obtain significant foreign intelligence or counterintelligence, or a delay in obtaining such information, that would result in substantial harm to national security.

2.6. (U) EXCEPTIONS.

a. (U) Counterdrug Activities and Activities to Counter Transnational Organized Crime.

~~(S//SI//REL)~~ Notwithstanding the limitations on targeting U.S. persons in Paragraphs 2.5.a. and b., the USSS may target [redacted] U.S. persons outside the United States who are suspected of involvement in international narcotics trafficking or transnational organized crime. This exception only applies where the communicants do not have a reasonable expectation of privacy in such radio communications and the communications are not otherwise protected by the Fourth Amendment.

b. (U) Illicit Communications.

(U) Notwithstanding the prohibition on collecting domestic communications in Paragraph 2.4.a. and the limitations on collection in Paragraph 2.5, the USSS may, for a period of time not to exceed 90 days and for the purpose of acquiring significant foreign intelligence or counterintelligence, collect communications with the specific prior approval of the Attorney General based on the Attorney General's determination that there is probable cause to believe that both of the following apply:

(1) (U) The communications have been transmitted in violation of either the Communications Act of 1934, as amended, and regulations issued thereunder, or international agreements, and

(2) (U) Because of their explicit content, message characteristics, or method of transmission, the communications are to or from an agent or agents of foreign powers, whether or not U.S. persons.

SECTION 3: (U) PROCESSING AND QUERYING

3.1. (U) SCOPE.

(U) This section governs processing of SIGINT and establishes requirements for querying unevaluated SIGINT in addition to the requirements of Paragraphs 3.3.f.(1) and 3.3.g.(2) of DoDM 5240.01.

3.2. (U) PROCESSING.

(U) The USSS may process SIGINT to prepare data for analysis. SIGINT collected by the USSS or other authorized entities, including foreign cryptologic partners, may be forwarded to NSA or intermediate processing facilities.

a. (U) Examples of processing activities that may be undertaken by the USSS include:

(1) (U) Processing information to characterize or understand signals and communications.

(2) (U) Taking all steps necessary to convert information into an intelligible form intended for human inspection, including decryption or cryptanalysis.

(3) (U) Reverse engineering malicious signals or potential malware.

(4) (U) Combining SIGINT information with other information to facilitate activities such as data correlation, retrieval, formatting, and conversion.

(5) (U) Identifying or labeling information for more efficient analysis.

(6) (U) Processing information to limit USPI and non-pertinent information as set out in Paragraph 2.3.

b. (U) If, in the course of processing activities, the contents of communications are retrieved for human inspection, such as for determining whether the information meets foreign intelligence, counterintelligence, or support to military operations requirements, such activities must comply with the querying provisions of this section.

3.3. (U) QUERYING.

(U) The USSS may conduct queries of communications authorized for collection for foreign intelligence, counterintelligence, and support to military operations purposes, and for the purpose of protecting the safety or enabling the recovery of a U.S. person reasonably believed to be held captive outside the United States by a foreign power or other non-U.S. person. Queries using selection terms that are reasonably likely to result in, or have resulted in, the retrieval of communications to, from, or about a U.S. person will be designed to defeat, to the extent

practicable under the circumstances, the retrieval of those communications, or data related to such communications, not relevant to the purposes specified above. If a query produces a communication subject to Paragraph 4.6, the USSS must handle the communication in accordance with that section.

3.4. (U) LIMITATIONS ON QUERYING.

(U) The USSS may conduct queries intended to retrieve foreign communications to, from, or about a U.S. person or a person located in the United States only if one of the following circumstances exists:

a. (U) Consent.

(U) The USSS may conduct queries intended to retrieve foreign communications to, from, or about a U.S. person or a person located in the United States if the person, or a third party (i.e., an individual or organization) who is legally authorized to consent on behalf of the person, has provided an appropriate consent on a case-by-case basis.

b. (U) Current FISA Targets.

(U) The USSS may conduct queries intended to retrieve foreign communications to, from, or about a U.S. person or a person located in the United States if the subject of the query has been determined to be an agent, officer, or employee of a foreign power authorized for electronic surveillance, physical search, or an acquisition pursuant to Sections 105, 304, 703, 704, or 705 of FISA (Sections 1805, 1824, 1881b-d of Title 50, U.S.C.) at the time such query is to be conducted. If there is any question whether the subject of a query is a currently authorized target of such an order or authorization, the compliance organization or legal counsel of the USSS element must consult with NSA OGC. NSA OGC will further coordinate, as needed, with the Office of Intelligence of the National Security Division, Department of Justice.

c. (U) Cyber Threat Activity.

~~(S//REL)~~ The USSS may conduct queries using a selection term that is intended to retrieve foreign communications to, from, or about a U.S. person or a person located in the United States [redacted] cyber threat activity of foreign actors. Queries conducted under this provision must comply with USSS internal policy approved by the DIRNSA.

d. ~~(S//REL)~~ Individuals or Entities [redacted]

~~(S//SI//REL)~~ The USSS may conduct queries intended to retrieve foreign communications to, from, or about an individual or entity [redacted] when USSS personnel have confirmed that the subject of the query [redacted] of a foreign power in the United States.

e. (U) Queries Concerning a Target Physically Entering the United States.

(U) The USSS may conduct queries intended to retrieve foreign communications to, from, or about a non-U.S. person who enters the United States if at the time of entering the United States the person was a target of collection and if circumstances suggest that the person is an agent of a foreign power. Such querying may be conducted for a period not to exceed 72 hours after the USSS learns that the non-U.S. person has entered and is in the United States. Such querying may continue beyond 72 hours if the USSS has or obtains authorization for querying under other provisions of this section.

f. (U) DIRNSA Approval.

(U) With the specific approval of the DIRNSA or a delegee (except for Paragraph 3.4.f.(4)):

(1) (U) U.S. Persons Held Captive Outside the United States.

(U) The USSS may conduct queries intended to retrieve foreign communications to, from, or about a U.S. person who is reasonably believed to be held captive outside the United States by a foreign power or other non-U.S. person for the purpose of protecting the safety or enabling the recovery of that captive. NSA OGC will promptly notify the National Security Division of the Department of Justice of use of this authority.

(2) (U) Exigent Circumstances.

(U) The USSS may conduct queries intended to retrieve foreign communications to, from, or about a U.S. person or a person located in the United States when a person's life or physical safety or the physical security of a defense installation or government property is reasonably believed to be in imminent danger to identify or develop information about that imminent danger. NSA OGC will, within 72 hours, notify the National Security Division of the Department of Justice and the Office of the Under Secretary of Defense for Intelligence and Security of use of this authority. Such querying may not continue for more than 72 hours unless the use is authorized under another provision of this section, such as Paragraph 3.4.g.(2).

(3) (U) Non-U.S. Persons in the United States.

(U) The USSS may conduct queries intended to retrieve foreign communications to, from, or about a non-U.S. person located in the United States if either of the following circumstances exists:

(a) (U) The query is limited to communications obtained at times when the person is reasonably believed to have been outside the United States.

(b) ~~(S//SI//REL)~~ The subject of the query [redacted] of a foreign power, as that term is defined at Paragraphs (1) - (3) of the Glossary's definition of a "foreign power," or a business entity in the United States that is openly acknowledged to be directed and controlled by a foreign government or governments. Queries conducted under this provision must comply with USSS internal policy approved by the DIRNSA.

(4) (U) Particular Foreign Power Datasets.

(U) With the approval of the DIRNSA, for a period not to exceed one year, the USSS may conduct queries against particular foreign power datasets intended to retrieve foreign communications about a U.S. person or a person in the United States (rather than communications to or from such a person), if all of the following conditions are met:

(a) (U) There is specific information indicating that the U.S. person, or the person in the United States, is the target or possible agent of a foreign power.

(b) (U) The purpose of the query is to retrieve significant foreign intelligence or counterintelligence information or to support military operations.

(c) (U) There is a high likelihood, based on the nature of the dataset, that any USPI included in the dataset would constitute foreign intelligence, counterintelligence, or information needed to support military operations.

g. (U) Attorney General Approval.

(U) With the approval of the Attorney General, for a period not to exceed 90 days:

(1) (U) Agent of a Foreign Power.

(U) The USSS may conduct queries using a selection term intended to retrieve foreign communications to, from, or about a U.S. person or a person in the United States if both of the following conditions are met:

(a) (U) There is probable cause to believe that the person is an agent of a foreign power or an officer or employee of a foreign power.

(b) (U) The purpose of the query is to acquire significant foreign intelligence or counterintelligence information.

(2) (U) Protection from Threats.

(U) The USSS may conduct queries intended to retrieve foreign communications to, from, or about a U.S. person or a person located in the United States for the purpose of identifying or developing information about one or more of the following circumstances:

(a) (U) A person's life or physical safety or the physical security of a defense installation or government property is reasonably believed to be in imminent danger.

(b) (U) The subject of the query is reasonably believed to be planning, or involved in planning, an assassination, kidnapping, terrorist attack, mass casualty attack, or significant cyber incident.

(c) (U) The subject of the query is reasonably believed to have participated in an actual or attempted assassination, kidnapping, terrorist attack, mass casualty attack, or significant cyber incident, and it is important to determine whether a foreign power may be involved.

(d) (U) The subject of the query is reasonably believed to have a foreign connection, and the purpose of the query is to:

1. (U) Protect a person's life or physical safety, or the physical safety of a defense installation or government property;

2. (U) Protect critical infrastructure from significant harm or disruption;

3. (U) Protect against international terrorist activities; or

4. (U) Protect classified or national defense information.

(3) (U) Particular Foreign Power Datasets.

(U) The USSS may conduct queries against particular foreign power datasets intended to retrieve foreign communications to, from, or about a U.S. person or a person in the United States, if all of the following conditions are met:

(a) (U) There is specific information indicating that the U.S. person, or the person in the United States, is the target or possible agent of a foreign power.

(b) (U) The purpose of the query is to retrieve significant foreign intelligence or counterintelligence information or to support military operations.

(c) (U) There is a high likelihood, based on the nature of the dataset, that any USPI included in the dataset would constitute foreign intelligence, counterintelligence, or information needed to support military operations.

3.5. (U) EXCEPTION FOR COMMUNICATIONS METADATA ANALYSIS.

(U) The USSS may conduct communications metadata analysis, including contact chaining, only for valid, documented foreign intelligence, counterintelligence, or support to military operations purposes or for the purpose of protecting the safety or enabling the recovery of a U.S. person reasonably believed to be held captive outside the United States by a foreign power or other non-U.S. person. Notwithstanding Paragraphs 3.3 and 3.4, it may engage in these activities without regard to the physical location or nationality of any of the communicants or the location or registration of any device.

SECTION 4: (U) RETENTION

4.1. (U) SCOPE.

(U) Procedure 3 of DoDM 5240.01 governs the retention of USPI. This section (i) modifies the retention periods for SIGINT information to the extent that the retention periods conflict with Paragraphs 3.3.c. and 3.3.e. of DoDM 5240.01, and (ii) implements Section 309 of the Intelligence Authorization Act for Fiscal Year 2015 (Section 1813 of Title 50, U.S.C.) in greater detail than DoDM 5240.01.

4.2. (U) RETENTION OF UNEVALUATED SIGINT.

(U) The USSS may retain unevaluated SIGINT for up to 5 years from the time it is collected. The USSS may retain unevaluated SIGINT that is enciphered or reasonably believed to have a secret meaning for sufficient duration to permit exploitation. To the extent practicable, unintelligible information will be processed into an intelligible form. For any unevaluated SIGINT that is enciphered or reasonably believed to have a secret meaning, the 5-year retention period begins when the unevaluated SIGINT is processed into intelligible form.

4.3. (U) EXTENDED RETENTION OF UNEVALUATED SIGINT.

(U) The DIRNSA may approve, in accordance with other applicable policies and guidance, either at the time of collection or thereafter, the retention of unevaluated SIGINT for up to an additional 20 years beyond the default retention period. The DIRNSA may approve such extended retention if the DIRNSA determines that such retention is necessary to protect the national security of the United States and submits a written certification to the congressional intelligence committees describing:

a. (U) The reasons extended retention is necessary to protect the national security of the United States.

b. (U) The duration for which retention is extended.

c. (U) The particular information to be retained.

d. (U) The measures the USSS is taking to protect the privacy interests of U.S. persons or persons located in the United States.

4.4. (U) AUTHORIZED RETENTION PERIODS FOR EVALUATED SIGINT.

(U) The USSS may retain the following categories of evaluated SIGINT in its original or transcribed form as specified below:

a. (U) Foreign Communications that Do Not Contain USPI.

(U) The USSS may permanently retain foreign communications that are determined to constitute, in whole or in part, foreign intelligence or counterintelligence, or information necessary to understand or assess foreign intelligence or counterintelligence, and in which all parties to the communication are reasonably believed to be non-U.S. persons, and from which any USPI has been removed.

b. (U) Foreign Communications that Contain USPI.

(U) The USSS may retain foreign communications to, from, or about a U.S. person in excess of 5 years in any of the following circumstances:

(1) (U) Foreign Intelligence.

(U) A communication that contains USPI may be retained permanently if it has been affirmatively determined, in whole or in part, to constitute foreign intelligence or counterintelligence, or information necessary to understand or assess foreign intelligence or counterintelligence.

(2) (U) Certain Information Necessary to Understand or Assess Foreign Intelligence or Counterintelligence.

(U) Communications necessary to understand or assess foreign intelligence or counterintelligence, such as for use in cryptanalysis, may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation and may consist of any period of time required for the above-stated purposes. If USPI does not need to be retained for these purposes, it will be deleted or replaced by a generic term when practicable.

(3) (U) Threat to Life.

(U) A communication necessary to protect against an imminent threat to human life may be retained in excess of 5 years. If information is being retained pursuant to this paragraph, both the nature of the threat and the information to be retained must be reported to the congressional intelligence committees not later than 30 days after the date such retention is extended.

(4) (U) Technical Assurance and Compliance Information.

(U) A communication necessary for technical assurance or compliance purposes may be retained in excess of 5 years. Any retention beyond 5 years must be reported annually to the congressional intelligence committees and the DoD Senior Intelligence Oversight Official. Examples of technical assurance and compliance information include the limited exceptions indicated in Paragraph 1.3.f.

4.5. (U) RETENTION OF COMMUNICATIONS METADATA.

(U) The USSS may permanently retain communications metadata and the associated metadata analysis, e.g., contact chaining, that is affirmatively determined, in whole or in part, to be foreign intelligence or counterintelligence information, or information necessary to understand or assess foreign intelligence or counterintelligence. Any communications metadata that contains USPI and does not meet the requirements for permanent retention under this paragraph may only be retained in excess of 5 years in accordance with the requirements for extended retention of unevaluated SIGINT as indicated in Paragraph 4.3 or the requirements for technical assurance and compliance information as indicated in Paragraph 4.4.b.(4).

4.6. (U) DESTRUCTION REQUIREMENTS.

a. (U) Destruction of Domestic Communications.

(U) The USSS may not retain domestic communications in which a person has a reasonable expectation of privacy and a warrant would be required to collect the communications for law enforcement purposes, unless the Attorney General determines that the retention is lawful and the contents indicate a threat of death or serious bodily harm to any person.

b. (U) Additional Destruction Requirement for Communications of U.S. Persons.

(U) In addition to complying with the destruction requirement in Paragraph 4.6.a., the USSS will take steps, to the extent practicable under the circumstances, to destroy promptly upon recognition any communications acquired by the USSS as the result of the inadvertent targeting of a non-consenting U.S. person. The destruction of such communications may be waived by the DIRNSA or a delegee if all of the following conditions are met:

(1) (U) FISA does not preclude their retention.

(2) (U) Their retention is consistent with the requirements of Paragraphs 4.2 through 4.5.

(3) (U) The DIRNSA or a delegee determines that the communications contain evidence of a crime or significant foreign intelligence or counterintelligence, or indicate a threat of serious harm to life or property.

c. (U) Additional Destruction Requirement for Communications of Certain Non-U.S. Persons.

~~(S//SI//REL)~~ In addition to complying with the destruction requirement in Paragraph 4.6.a. and the other requirements for retention under Paragraphs 4.2 through 4.5, the USSS will take steps, to the extent practicable under the circumstances, to destroy communications (i) that were acquired by the USSS as a result of the inadvertent targeting of a non-consenting, [redacted] in the United States at the time of collection, and (ii) that do not otherwise contain evidence of a crime or significant foreign intelligence or counterintelligence, or indicate a threat of serious harm to life or property.

SECTION 5: (U) DISSEMINATION

5.1. (U) SCOPE.

(U) This section governs the dissemination of USPI derived from SIGINT activities conducted in accordance with this annex. The dissemination of USPI and information derived from SIGINT must also comply with the requirements of Procedures 4 and 5 of DoDM 5240.01.

5.2. (U) MINIMIZATION OF USPI IN DISSEMINATIONS.

(U) The USSS may not include USPI in a SIGINT dissemination unless one or more of the following conditions is met and an authorized USSS official determines that the recipient is reasonably believed to have a need for the USPI for the performance of its lawful missions or functions:

a. (U) Consent.

(U) The U.S. person whom the information concerns, or a third party (i.e., an individual or organization) who is legally authorized to consent on behalf of such person, has provided an appropriate consent on a case-by-case basis.

b. (U) Publicly Available.

(U) The USPI is publicly available information.

c. (U) Foreign Intelligence or Counterintelligence.

(U) The USPI is necessary for the intended recipients to understand the foreign intelligence or counterintelligence information to which the USPI pertains or to assess its importance. The following nonexclusive list contains examples of the types of foreign intelligence or counterintelligence information that would meet this standard and justify the dissemination of the USPI:

(1) (U) The foreign intelligence or counterintelligence information indicates that the U.S. person may be a foreign power, an agent of a foreign power, or an officer or employee of a foreign power.

(2) (U) The foreign intelligence or counterintelligence information indicates that the USPI may be pertinent to the unauthorized disclosure of classified information, including such disclosure by U.S. persons.

(3) (U) The foreign intelligence or counterintelligence information indicates that the USPI may be pertinent to international narcotics trafficking activities, including such activities by U.S. persons.

(4) (U) The foreign intelligence or counterintelligence information indicates that the USPI may be pertinent to hostile intelligence activities of a foreign power, including U.S. persons who are targets of or involved in hostile intelligence activities.

(5) (U) The foreign intelligence or counterintelligence information may be pertinent to a possible threat to the safety of any person or organization, including those who are targets, victims, or hostages of international terrorist organizations, or targets or victims of foreign cyber threat activity or cybercrime.

(6) (U) The foreign intelligence or counterintelligence information indicates that the U.S. person is a senior official of the Executive Branch of the U.S. Government. In this case, only the official's title will be disseminated. When this exemption is applied, the DIRNSA or a delegee will ensure that domestic political or personal information that is not necessary to understand foreign intelligence or counterintelligence or assess its importance is not disseminated.

d. (U) Evidence of a Crime.

(U) The information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that both of the following apply:

(1) (U) The dissemination is for law enforcement purposes.

(2) (U) The dissemination is reported as provided in the August 22, 1995 DoD and Department of Justice Memorandum of Understanding on Reporting of Information Concerning Federal Crimes, or other applicable memorandums of understanding or successor documents.

e. (U) U.S. Person Captive.

(U) The dissemination is for the purpose of protecting the safety or enabling the recovery of a U.S. person reasonably believed to be held captive outside the United States by a foreign power or other non-U.S. person.

f. (U) Required Disseminations.

(U) The dissemination is required by statute; treaty; E.O.; Presidential directive; National Security Council directive; or policy, memorandum of understanding, or agreement approved by the Attorney General.

5.3. (U) INFORMATION OBTAINED FROM SURVEYS.

a. (U) Information necessary for cataloging the constituent elements of the signals environment may be disseminated to the extent such information is not USPI. Communications equipment nomenclature may be disseminated regardless of whether it may be USPI.

b. (U) Information that reveals a vulnerability to U.S. Government or allied nations' communications security may be disseminated to the appropriate communications security authorities.

SECTION 6: (U) POLICY, OVERSIGHT, AND TRAINING

6.1. (U) SCOPE.

(U) This section governs activities undertaken by the USSS to ensure compliance with the requirements of this annex and DoDM 5240.01 in order for the USSS to conduct authorized activities in a manner that protects the constitutional and other legal rights of U.S. persons and persons in the United States as well as the privacy and civil liberties of such persons.

6.2. (U) INTERNAL POLICIES.

(U) The DIRNSA, as head of the USSS, will issue appropriate policies implementing this annex in coordination with legal, civil liberties, and privacy officials, who will also oversee policy implementation. Internal policies will cover implementation of the collection, processing, querying, retention, dissemination, and training requirements identified in this annex.

6.3. (U) COMPLIANCE PROGRAMS.

(U) The DIRNSA will develop and maintain internal compliance, training, and auditing programs. These programs will be designed to:

a. (U) Implement the training and auditing required by Paragraphs 6.4 and 6.5.

b. (U) Ensure that USSS personnel who have been granted access to unevaluated SIGINT continue to require such access.

c. (U) Ensure that the USSS collects, processes, queries, retains, and disseminates SIGINT in accordance with Sections 2 through 5.

d. (U) Comply with the requirements of DoDM 5240.01, including this annex, and DoD issuances governing oversight and compliance, such as DoDD 5148.13, or successor guidance.

6.4. (U) TRAINING.

(U) All USSS personnel who have access to unevaluated SIGINT will receive training on DoDD 5148.13 and DoDM 5240.01, including the requirements for collecting, processing, querying, retaining, and disseminating information subject to this annex, as appropriate. Other USSS personnel whose duties require them to comply with provisions of this annex will also receive appropriate training.

6.5. (U) AUDITING AND INTERNAL CONTROLS.

(U) The USSS will audit SIGINT activities conducted pursuant to this annex. It will create and maintain sufficient auditing records to verify compliance with the requirements of this annex and

protect auditing records against unauthorized access, modification, or deletion. The USSS will periodically review the effectiveness of its auditing. The auditing and internal controls must address all of the following minimum requirements:

a. (U) Collection.

(U) The USSS will document and annually review the use of selection terms as the basis for collection to ensure compliance with the provisions of Section 2.

b. (U) Access.

(U) Access to unevaluated SIGINT will be recorded and reviewed by supervisory or other appropriate personnel.

c. (U) Queries.

(U) Queries will be reviewed, to the extent reasonably practicable, through the use of methods (e.g., automated sampling, spot checks, or human inspection) approved after consultation with legal, civil liberties, and privacy officials. The USSS will determine the appropriate periodicity and scope of audits on the basis of the sensitivity of the particular category of SIGINT information at issue and the likelihood of an improper query or other improper use of SIGINT.

d. (U) Retention and Dissemination.

(U) The USSS will review the retention and dissemination of USPI to ensure compliance with the provisions of Sections 4 and 5.

6.6. (U) REPORTING.

a. (U) Annual Report on Communications Metadata.

(U) On an annual basis, NSA will report all of the following to the National Security Division of the Department of Justice with copies to the Offices of the Under Secretary of Defense for Intelligence and Security, the General Counsel of the Department of Defense, the DoD Senior Intelligence Oversight Official, and the DNI:

(1) (U) The kinds of information that the USSS is collecting, processing, querying, and retaining as communications metadata.

(2) (U) The USSS's implementation of the protections required by this annex for the communications metadata of U.S. persons.

(3) (U) Any significant new legal or oversight issues, even if already reported in the current reporting period, that have arisen in connection with the collection, processing, querying, retention, or dissemination of the communications metadata of U.S. persons.

b. (U) Other Reports.

(U) NSA will report any of the following to the National Security Division of the Department of Justice, with copies to DoD OGC and ODNI:

(1) (U) Substantial changes in any collection authorized under Paragraph 2.5.a.(1)(b), including changes to the purpose or targets of the collection or the minimization procedures being applied, and the termination of the collection.

(2) (U) Any circumstance in which collection should have been approved by the DIRNSA or a delegee or the Attorney General under Paragraphs 2.5 or 2.6, or FISA, but was not.

(3) (U) Any circumstance in which a query should have been approved by the DIRNSA or a delegee or the Attorney General under Paragraph 3.4., but was not.

c. (U) Reports to the Department of Defense.

(U) NSA will also provide all reports required by DoDD 5240.01, DoDD 5143.01, and DoDD 5148.13.

SECTION 7: (U) CERTAIN U.S. PERSON FISA TARGETS OUTSIDE THE UNITED STATES

(U) SCOPE.

(U) The attached appendix pertains to U.S. persons outside the United States targeted under Section 2.5 of E.O. 12333 and Section 704, 705(b), or 705(c) of FISA.

APPENDIX 7A: (U) U.S. PERSON TARGETS OUTSIDE THE UNITED STATES UNDER SECTION 2.5 OF E.O. 12333 AND SECTION 704, 705(B), OR 705(C) OF FISA

7A.1. (U) GENERAL.

a. (U) This appendix applies to USSS implementation of techniques for targeting a U.S. person outside the United States pursuant to Section 704, 705(b), or 705(c) of FISA in conjunction with Section 2.5 of E.O. 12333. As relevant to this appendix, Section 2.5 of E.O. 12333 delegates to the Attorney General the power to approve the use for intelligence purposes against a U.S. person abroad of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that the Attorney General finds in each case probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. When the Attorney General approves an application or authorizes an emergency acquisition under Section 704, 705(b), or 705(c) of FISA, the Attorney General is also concurrently approving the use of a technique required for such targeting consistent with Section 2.5 of E.O. 12333. As used in this appendix and Section 2.5 of E.O. 12333, the term "agent of a foreign power" includes a U.S. person abroad who is an officer or employee of a foreign power.

b. (U) Activities conducted under FISA are subject to orders of the Foreign Intelligence Surveillance Court (FISC), authorizations from the Attorney General, certifications under Section 702 of FISA, and related targeting, querying, and minimization procedures. Nothing in this appendix is intended to limit the requirements or applicability of FISA.

c. (U) This appendix replaces the Letter to Keith B. Alexander, Director of NSA, from Attorney General Michael Mukasey (August 18, 2008), regarding the implementation of certain amendments to FISA.

7A.2. (U) SECTIONS 704, 705(B), AND 705(C) OF FISA.

(U) Section 704 of FISA permits the FISC (or, in an emergency, the Attorney General) to authorize an acquisition targeting a U.S. person outside the United States. Similarly, when the FISC (or, in an emergency, the Attorney General) authorizes electronic surveillance or a physical search of a U.S. person under Section 105 or 304 of FISA, Sections 705(b) and 705(c) permit the Attorney General to authorize the targeting of the U.S. person when he or she is outside the United States.

7A.3. (U) AUTHORIZED TIME PERIODS FOR ACQUISITIONS UNDER SECTIONS 704, 705(B), AND 705(C).

(U) When the Attorney General approves the use by the USSS for intelligence purposes against a U.S. person abroad of a technique that requires approval under Section 2.5 of E.O. 12333, the USSS may engage in such acquisition:

a. (U) Section 704.

(U) Only for the time period authorized by the FISC or the Attorney General under Section 704 and for such time as the target is reasonably believed to be outside the United States.

(1) (U) If the target is reasonably believed to be in the United States, the USSS shall cease any acquisition under this section unless the target is again reasonably believed to be outside the United States.

(2) (U) In addition, if the Attorney General has approved an emergency authorization, the acquisition shall terminate when the information sought is obtained, if the application for a FISC order is denied, or 7 days from the time of the authorization, whichever is earliest.

b. (U) Section 705(b).

(U) Only for the time period authorized by the FISC (in the order under Section 105 or 304) and for such time as the target is reasonably believed to be outside the United States. If the target is reasonably believed to be in the United States, the USSS shall cease any acquisition under this section unless the target is again reasonably believed to be outside the United States.

c. (U) Section 705(c).

(U) Only for the time period authorized by the Attorney General or the FISC (in the emergency authorization and subsequent order, if any, under Section 105 or 304) and for such time as the target is reasonably believed to be outside the United States.

(1) (U) If the target is reasonably believed to be in the United States, the USSS shall cease any acquisition under this section unless the target is again reasonably believed to be outside the United States.

(2) (U) In addition, in the absence of a subsequent FISC order approving the acquisition, the acquisition shall terminate when the information sought is obtained, if the application for a FISC order is denied, or 7 days from the time of the authorization, whichever is earliest.

7A.4. (U) COLLECTION TECHNIQUES.

(U) For an acquisition covered by Paragraph 7A.3., the USSS may use the following techniques, provided that the technique does not constitute "electronic surveillance" or a "physical search" as defined by FISA:

a. (U) Selection Term-Based Surveillance.

(U) The USSS may use any selection term intended to acquire foreign communications or other information to, from, or about the target.

b. (U) Computer Surveillance.

~~(S//SI//REL)~~ The USSS may acquire

(1) ~~(S//SI//REL)~~ Communications or information of or concerning the target

(2) ~~(S//SI//REL)~~ Information of or concerning the target that may be obtained

a non-U.S. person reasonably believed both to be outside the United States and to possess or communicate information of or concerning the target.

c. (U) Other Techniques.

(U) The USSS may use any other technique approved by the Attorney General.

d. (U) Use of Techniques.

(U) In developing and implementing the collection techniques authorized in paragraphs 7A.4.a through 7A.4.c, the USSS, consistent with mission requirements and internal policy, will consider (1) methods to limit the collection of USPI that does not relate to the target or is not relevant to the purpose of the collection, and (2) whether mission requirements can be met by filtering non-pertinent information as soon as practicable after collection.

7A.5. (U) REVERSE TARGETING.

(U) The USSS will not intentionally collect foreign communications or other information for the purpose of targeting a specific U.S. person unless such U.S. person has been separately authorized for targeting in the manner prescribed by this appendix. Thus, the USSS may target a non-U.S. person outside the United States in order to collect information to, from, or about a U.S. person authorized for targeting under this appendix. In using the techniques referenced in Paragraph 7A.4, the USSS will consult with the Office of Intelligence of the National Security Division, Department of Justice, if a collection activity would appear to constitute reverse targeting of a U.S. person other than an authorized target.

7A.6. (U) GOVERNING AUTHORITIES.

(U) The applicable FISC order or emergency authorization and associated minimization procedures govern the acquisition, processing, querying, retention, and dissemination of information acquired under Section 704, 705(b), or 705(c).

7A.7. (U) DISCLOSURE FOR LAW ENFORCEMENT PURPOSES.

(U) No information acquired under Section 704, 705(b), or 705(c) will be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived from that acquisition, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

7A.8. (U) REPORTING.

(U) If the USSS conducts an acquisition against a U.S. person under Section 704, 705(b), or 705(c) while that person is inside the United States, NSA must report such acquisition to the Department of Justice through the Deputy Assistant Attorney General of the National Security Division responsible for intelligence operations and oversight within 7 days. In addition NSA will report to the National Security Division, upon request, the name of each target as to which NSA conducted an acquisition under Section 704, 705(b), or 705(c).

7A.9. (U) ADDITIONAL PROCEDURES FOR FEDERAL BUREAU OF INVESTIGATION (FBI)-NOMINATED TARGETS AND CURRENT FBI FISA TARGETS.

(U) When the USSS conducts an acquisition under Section 704 requested by the FBI, or under Section 705(b) or 705(c) granted in conjunction with an FBI FISA authorization under Section 105 or 304:

a. (U) Coordination Before Acquisition.

(U) Before commencing acquisition, the USSS must:

(1) (U) Confirm with the FBI that the target is reasonably believed to be outside the United States. Except in exigent circumstances, the USSS must obtain such confirmation in writing.

(2) (U) Obtain the expiration date of the FISC order and confirm that it remains in effect. Except in exigent circumstances, such confirmation must be in writing.

b. (U) Coordination After Initiation of Acquisition.

(U) During any period of acquisition, the USSS must:

(1) (U) Coordinate with the FBI in a manner designed to ensure that the USSS is made aware, in a timely way, of any information indicating that the target has returned, or plans to return, to the United States. The Attorney General has directed the FBI to share with NSA, as promptly as practicable, any information it may have that a target of an acquisition authorized under Section 704, 705(b), or 705(c) has returned, or plans to return, to the United States, including the known or anticipated dates of travel.

(2) (U) Periodically re-confirm with the FBI, as needed, that the FBI reasonably believes the target remains outside the United States.

7A.10. (U) QUESTIONS ABOUT FISA MATTERS.

a. (U) The compliance organization or legal counsel of the appropriate USSS element will consult with NSA OGC if there is any question:

(1) (U) About a FISA order or authorization;

(2) (U) Whether authorization under FISA may be required; or

(3) (U) Whether a Section 704, 705(b), or 705(c) acquisition must cease in light of information indicating that the target has entered the United States.

b. (U) NSA OGC will further coordinate with the Office of Intelligence of the National Security Division, Department of Justice, as needed.

(U) GLOSSARY

This Glossary is UNCLASSIFIED

G.1. (U) ACRONYMS.

ACRONYM	MEANING
COMINT	communications intelligence
DIRNSA/CHCSS	Director of the National Security Agency/Chief of the Central Security Service
DNI	Director of National Intelligence
DoDD	DoD directive
DoDM	DoD manual
ELINT	electronic intelligence
E.O.	Executive order
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FISINT	foreign instrumentation signals intelligence
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OGC	Office of the General Counsel
SIGINT	signals intelligence
U.S.C.	United States Code
USPI	U.S. person information
USSS	United States SIGINT System

G.2. (U) DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
agent of a foreign power	1 Any person, other than a U.S. person, who: a. Acts in the United States as an officer or employee of a foreign power, or as a member of a group engaged in

TERM	DEFINITION

international terrorism or activities in preparation therefor, irrespective of whether the person is in the United States;

b. Acts for, or on behalf of, a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances indicate that such person may engage in such activities, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

c. Engages in international terrorism or activities in preparation therefor;

d. Engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

e. Engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefor; or

2 Any person, including a U.S. person, who:

a. Knowingly engages in clandestine intelligence gathering activities for, or on behalf of, a foreign power, which activities involve, or may involve, a violation of the criminal statutes of the United States;

b. Pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for, or on behalf of, such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

c. Knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

d. Knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or,

TERM	DEFINITION
	while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or e. Knowingly aids or abets any person in the conduct of activities described in Paragraphs 2.a through 2.c or knowingly conspires with any person to engage in those activities.
Attorney General	The Attorney General, the Acting Attorney General, the Deputy Attorney General, or the Assistant Attorney General for National Security.
bulk collection	The collection of data that, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.).
collection	Defined in DoDM 5240.01.
communicant	A sender or intended recipient of a communication.
communications metadata	1. The dialing, routing, addressing, or signaling information associated with a communication — whether such communication occurs between two or more persons, between devices or infrastructure used to route communications to and from the communicants, or is a machine-to-machine communication — but does not include information concerning the substance, purport, or meaning of the communication. 2. Communications metadata includes, for example, the following types of metadata: a. Telephony metadata includes addressing information such as the telephone number of the calling party and the telephone number of the called party, as well as the date, time, and duration of the call. b. For electronic communications: (1) Metadata includes addressing information, such as the information appearing on the "to," "from," "cc," and "bcc" lines of a standard e-mail or other electronic communication. For e-mail communications, the "from" line contains the e-mail address of the sender,

TERM	DEFINITION
	and the "to," "cc," and "bcc" lines contain the e-mail addresses of the recipients. Metadata also includes: (a) Information about the Internet protocol addresses of the computers sending and receiving an e-mail or other electronic communication and, depending on the circumstances, about the Internet protocol addresses of routers and servers on the Internet that have handled the communication during transmission. (b) The exchange of an Internet protocol address and e-mail address that occurs when a user logs into a web-based e-mail service. (c) For certain logins to web-based e-mail accounts, mailbox metadata that is transmitted to the user upon accessing the account. (2) Metadata associated with electronic communications does not include information from the "subject" or "re" line of an e-mail or information from the body of an e-mail. Metadata also does not include domain name information beyond the fully qualified domain name.
communications security	Defined in DoDM 5240.01.
consent	Defined in DoDM 5240.01.
contact chaining	A process by which communications metadata is organized. It shows, for example, the telephone numbers or e-mail addresses that a particular telephone number or e-mail address has been in contact with, or has attempted to contact. Through this process, computer algorithms automatically identify not only the first tier of contacts made by the seed telephone number or e-mail address, but also the further contacts made by the first tier of telephone numbers or e-mail addresses and so on.
counterintelligence	Defined in DoDM 5240.01.
direction-finding	A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept

TERM	DEFINITION
	receiver or ancillary equipment. Direction-finding does not include electronic surveillance as defined by FISA.
dissemination	Defined in DoDM 5240.01.
domestic communication	Any communication where the sender and all intended recipients are in the United States.
electronic surveillance	Defined in DoDM 5240.01.
evaluated SIGINT	Any SIGINT that has been determined to qualify for retention under Paragraph 4.4 or 4.5.
foreign communication	A communication that involves a sender or an intended recipient who is outside the United States.
foreign connection	Defined in DODM 5240.01.
foreign intelligence	Defined in DoDM 5240.01.
foreign power	1. A foreign government or any component thereof, whether or not recognized by the United States. 2. A faction of a foreign nation or nations, not substantially composed of U.S. persons. 3. An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments. 4. A group engaged in international terrorism or activities in preparation therefor. 5. A foreign-based political organization, not substantially composed of U.S. persons. 6. An entity that is directed and controlled by a foreign government or governments. 7. An entity not substantially composed of U.S. persons that is engaged in the international proliferation of weapons of mass destruction.

TERM	DEFINITION
incidental collection of communications	The collection of the communications of a person whose communications are not deliberately sought but are nonetheless collected. Such collection is considered incidental regardless of whether it is expected or reasonably anticipated to occur.
intelligence	Defined in DoDM 5240.01.
intelligence activities	Defined in DoDM 5240.01.
Intelligence Community and elements of the Intelligence Community	Defined in DoDM 5240.01.
intentional collection of communications	The collection of communications of a person whose communications are deliberately sought.
international terrorism or international terrorist activities	Defined in DoDM 5240.01.
publicly available information	Defined in DoDM 5240.01.
reasonable belief	Defined in DoDM 5240.01.
reasonable expectation of privacy	Defined in DoDM 5240.01.
retention	Defined in DoDM 5240.01.
selection term	The composite of individual terms used to effect or defeat the collection or querying of particular communications, information, or data of interest. It comprises the entire term or series of terms so used, but not any segregable term contained therein. A selection term limits, to the greatest extent reasonably practicable, the scope of the information sought, consistent with the purpose of the collection or query.
significant cyber incident	An event (or group of related events) occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers,

TERM	DEFINITION
	information, or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon, where such event (or group of related events) is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.
target	An individual or entity from whom or about whom information is deliberately sought. When used as a verb, "to target" means deliberately to collect information about an individual or entity, including communications to or from such individual or entity.
unevaluated SIGINT	Any SIGINT that has not been determined to qualify for retention under Paragraph 4.4. or 4.5. Unevaluated SIGINT also is referred to as raw SIGINT in other procedures, policies, and regulations.
United States	Defined in DoDM 5240.01.
U.S. person	Defined in DoDM 5240.01
USPI	Defined in DoDM 5240.01.
USSS	The organization unified under the DIRNSA/CHCSS's authority to conduct SIGINT. The USSS includes NSA and components of the Military Services (including the U.S. Coast Guard) that are authorized to conduct SIGINT activities and such other entities authorized by the Secretary of Defense or the DIRNSA to conduct SIGINT activities pursuant to Section 1.7(c)(2) of E.O. 12333. The USSS does not include foreign cryptologic partners. A DoD component is not to be considered part of the USSS with respect to its non-SIGINT activities, and such activities are not governed by this annex.

(U) REFERENCES

The reference titles cited in this section are UNCLASSIFIED

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended

DoD Directive 5148.13, "Intelligence Oversight," April 26, 2017

DoD Directive 5240.01, "DoD Intelligence Activities," August 27, 2007, as amended

DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 8, 2016

DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," June 30, 2014, as amended

DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections," June 30, 2014, as amended

Executive Order 12333, "United States Intelligence Activities," as amended

Fourth Amendment of the Constitution

Memorandum of Understanding Between the Department of Defense and Department of Justice, "Reporting of Information Concerning Federal Crimes," August 22, 1995

Office of the Director of National Intelligence, "Procedures for the Availability or Dissemination of Raw Signals Intelligence Information by the National Security Agency under Section 2.3 of Executive Order 12333 (Raw SIGINT Availability Procedures)," (January 3, 2017)

United States Code, Title 47 (Chapter 5 is also known as "the Communications Act")

United States Code, Title 50 (Chapter 36 is also known as "the Foreign Intelligence Surveillance Act (FISA)")

(U) This Annex Supersedes and Repeals:

"Classified Annex to Department of Defense Procedures Under Executive Order 12333," May 27, 1988, including all amendments, appendices, and supplemental procedures, which include:

- National Security Agency, "Appendix A to the Classified Annex to Department of Defense Procedures Under Executive Order 12333, Procedures for Monitoring Radio Communications of Suspected Narcotics Traffickers," December 21, 1984.
- Department of Defense, "Department of Defense Supplemental Procedures Governing Communications Metadata Analysis (SPCMA)," January 3, 2008. The SPCMA are replaced by Paragraph 3.5, which addresses communications metadata analysis.

The August 18, 2008 Letter to Keith B. Alexander, Director of NSA, from Attorney General Mukasey regarding the implementation of certain amendments to FISA