(U) 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)

~~Classified By: 2476680~~
~~Derived From: NSA/CSSM 1-52~~
~~Declassify On: 20411231~~

TABLE OF CONTENTS

(U) 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)

(U) INTRODUCTION

(U) Section 2.3 of Executive Order (E.O.) 12333 allows an Intelligence Community (IC) element (IC element) to disseminate information to other appropriate IC elements "for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it." For the dissemination of information derived from signals intelligence (SIGINT), section 2.3 requires that such information only be disseminated or made available in accordance with procedures established by the Director of National Intelligence (DNI) in coordination with the Secretary of Defense and approved by the Attorney General. The DNI is establishing these Procedures to implement this provision of section 2.3 and to govern the availability of unevaluated and/or unminimized SIGINT and associated data (hereinafter "raw SIGINT") to IC elements by the National Security Agency/Central Security Service (NSA/CSS, hereinafter "NSA").

(U) SECTION I – PURPOSE AND SCOPE

A. (U) Purpose. The purpose of these Procedures is to enable IC elements to conduct their national security missions more effectively by providing them with access to raw SIGINT from NSA, as authorized by section 2.3 of E.O. 12333, in a manner that complies with the Fourth Amendment and protects the privacy of U.S. persons.

B. (U) Exclusions. These Procedures do not apply to:

1. (U) *NSA's SIGINT activities*. SIGINT activities conducted by NSA under its authorities and SIGINT activities conducted by another element of the IC pursuant to a delegation of SIGINT authority under section 1.7(c)(2) of E.O. 12333.

2. (U) *FISA information*. Information that NSA acquires under the Foreign Intelligence Surveillance Act (FISA), as amended. Foreign Intelligence Surveillance Court orders, authorizations from the Attorney General, and related minimization procedures govern the acquisition, retention, and dissemination of such information. Questions about access to such information should be referred to the National Security Division of the Department of Justice and NSA's Office of General Counsel (OGC).

3. (U) *Finished reporting based on SIGINT*. The receipt and further processing by an IC element of finished reporting from NSA based on SIGINT.

4. (U~~//FOUO~~) *Other activities*. Disseminations of raw SIGINT, or data provided by NSA, pursuant to a joint program or arrangement lawfully conducted under applicable procedures approved by the Attorney General, including activities conducted pursuant to National Security Council Intelligence Directives No. 5 (NSCID-5) and No. 6 (NSCID-6) or successor documents, and disseminations under any Presidentially-authorized covert action program where NSA has been named as a supporting agency.

5. (U) *Non-U.S. persons*. SIGINT information that is exclusively about non-U.S. persons that is evaluated and disseminated under other authorities, except where otherwise stated. SIGINT information about non-U.S. persons is subject to Presidential Policy Directive 28 (PPD-28) and implementing procedures and any successor documents.

C. (U) No authorization to collect information. These Procedures do not authorize NSA or any other IC element to collect SIGINT or other information.

(U) SECTION II - REQUESTS FOR RAW SIGINT

A. (U) Access request from an IC element. NSA may provide raw SIGINT to an IC element only if the head of the IC element or a high-level designee makes a written request describing the raw SIGINT sought and stating whether the element wishes to conduct communications metadata analysis in accordance with section IV.F below. The request will address the following:

1. (U) *Use of information*. The IC element will explain how it will use the raw SIGINT, to include identifying the particular authorized foreign intelligence or counterintelligence missions or functions that are the basis for its request.

2. (U) *Value of information*. The IC element will describe how it expects the raw SIGINT to further such missions or functions in a significant way.

3. (U) *Other sources of information*. The IC element will explain why other sources reasonably available to it cannot provide the information the element expects to obtain from the raw SIGINT.

4. (U) *Access requirements.* The IC element will describe its access requirements (*e.g.*, the estimated number of analysts who will have access to the raw SIGINT and the time period that the element will retain the raw SIGINT).

5. (U) *Processing and dissemination*. The IC element will explain how it will process raw SIGINT and, if appropriate, disseminate the information obtained from it.

6. (U) *Protection of information*. The IC element will explain how it will safeguard the raw SIGINT, including limiting access to those personnel described in section III.B.5 and protecting all sensitive sources, methods, and activities, in a manner consistent with security requirements specified or agreed to by the Director, NSA (DIRNSA).

7. (U) *Attorney General procedures*. The IC element's personnel will comply with either (i) these Procedures or (ii) any alternative procedures covering sections III through VIII and later established by the DNI and approved by the Attorney General governing the availability of raw SIGINT. Alternative procedures may be established based on existing procedures and may apply to NSA as well as other IC elements. The DNI will establish any alternative procedures in coordination with the Secretary of Defense, after consulting with affected elements and after approval by the Attorney General.

8. (U) *Reporting*. The IC element will provide in a timely and complete way any reporting required by these Procedures, and, if the IC element is seeking an extension of its access to raw SIGINT, the IC element must have provided such reporting prior to approval of an extension.

9. (U) *Compliance and oversight*. The IC element will describe its compliance and oversight program, including addressing how that program will meet each of the requirements found in section VII.C.

10. (U) *PPD-28*. The IC element's personnel will comply with PPD-28, implementing policies, and any successor documents.

11. (U) *Consultation*. The official has consulted with legal counsel and the senior official designated or identified by the IC element head, pursuant to section E.2.b of ICD 107, as responsible for matters involving the protection of civil liberties and privacy.

B. (U) Notification of SIGINT information of interest. In the course of its operations, NSA may identify raw SIGINT of potential interest to an IC element. NSA may, on its own initiative, notify the IC element of the existence of such information. The IC element must follow the procedure in paragraph A to request that the information be made available to it.

C. (U) Evaluation of requests. A high-level NSA official designated by the DIRNSA will review requests for raw SIGINT covered by these Procedures. NSA will document its approval decisions in writing and include a statement explaining how the request fully

complies with paragraph A. If the request complies with the requirements of paragraph A, in deciding whether to approve a request, the reviewing official will also consider:

1. (U) *Reasonableness*. Whether approving the request is reasonable in light of all the circumstances known at the time of the evaluation of the request, including but not limited to:

a. (U) The information provided under paragraph A by the requesting IC element;

b. (U) The likelihood that NSA has raw SIGINT responsive to the request that it is able to make available;

c. (U) The importance of the information to the IC element, as explained in the request;

d. (U) The ability of the IC element to process and, if appropriate, further disseminate the information as compared to the ability of NSA or other IC elements already possessing the information to do so;

e. (U) The likelihood that sensitive U.S. person information (USPI) will be found in the information and, if known, the amount of such information;

f. (U) The potential for substantial harm, embarrassment, inconvenience, or unfairness to U.S. persons if the USPI is improperly used or disclosed;

g. (U) The time period for which the IC element intends to retain the information; and

h. (U) The safeguards that will be applied to the information.

(U) Nothing in this paragraph should be construed to require NSA to review or evaluate the raw SIGINT that has been requested by the IC element when assessing the reasonableness of the request.

2. (U) *Need for the information requested*. Whether NSA can reasonably meet the requesting IC element's needs by providing, when practicable, more limited access to the requested information, or whether NSA has information other than raw SIGINT that can meet the requesting element's needs.

3. (U) *Compliance and protection*. Whether, based on the request from the IC element and any other information available, the requesting element has the ability to comply with these Procedures and to protect and handle raw SIGINT properly.

D. (U) Approved requests.

1. (U) *Memorandum of agreement (MOA).* Before NSA makes raw SIGINT available to a requesting IC element, the element and NSA must execute an MOA governing the availability, retention, and use of the information. The MOA will describe the element's oversight and compliance procedures to address the requirements of section VII; any additional training, guidance, or other assistance to be provided by NSA; and measures to protect SIGINT sources and methods from unauthorized disclosure. The MOA requires the approval of appropriate high-level officials at the requesting element, NSA, and the ODNI (in coordination with Department of Defense (DoD)), based on a finding that the requesting IC element has satisfied the requirements of these Procedures. The term of the MOA, or any renewal of it, will not exceed three years.

2. (U) *Access request and approval documentation.* Each specific request for access to raw SIGINT that has been approved by NSA will be documented in an appendix to the MOA with the recipient element. Access requests will be reviewed at least every three years, unless a shorter period is otherwise required by the MOA or otherwise. Any renewal of access to raw SIGINT, or expansion of the information that the recipient IC element is seeking, will require the recipient element to make a new request for the renewal or for the additional information, respectively, in accordance with paragraph A above.

E. (U) Denied requests. NSA will return a denied request to the requesting IC element with an explanation. Reasonable efforts will be made to resolve disagreements between NSA and the requesting IC element in a timely manner. The requesting IC element may appeal an adverse decision to the DIRNSA's designee, and then to the DIRNSA absent resolution with the DIRNSA's designee. In the event a disagreement between NSA and another DoD IC element cannot be resolved, the issue will be referred to the Secretary of Defense, and in the event resolution still cannot be reached, the issue will be referred to the DNI. For all other IC elements, when resolution cannot be reached, the issue will be referred to the DNI. An official resolving any disagreement will apply the standards of paragraph C.

(U) SECTION III – PROTECTIONS FOR RAW SIGINT

A. (U) Access to information. NSA may choose to make raw SIGINT available (i) through NSA's systems; (ii) through a shared IC or other Government capability, such as a cloud-based environment; or (iii) by transferring some or all of the information to the recipient IC element's information systems. Only information that can be afforded appropriate handling, storage, retention, and access protections by the recipient IC element will be made available.

B. (U) General protections. Any IC element that obtains access to raw SIGINT under these Procedures will:

1. (U) *Fourth Amendment*. Take steps to ensure its processing, retention, and dissemination of the information complies with applicable requirements of the Fourth Amendment.

2. (U) *Compliance with law*. Ensure that IC element personnel with access to raw SIGINT abide by the Constitution, applicable law, executive order, directive, regulation, policy, or guidance, including E.O. 12333, these Procedures, and the applicable MOA.

3. (U) *Political process in the United States*. Not engage in any intelligence activity authorized by these Procedures, including disseminations to the White House, for the purpose of affecting the political process in the United States. The IC element will comply with the guidance applicable to NSA regarding the application of this prohibition. Questions about whether a particular activity falls within this prohibition will be resolved in consultation with the element's legal counsel and the General Counsel of the Office of the Director of National Intelligence (ODNI) (and the DoD's Office of the General Counsel in the case of a DoD IC element).

4. (U) *Change in need for SIGINT*. Notify NSA of changes in its mission need and, if necessary, notify NSA that raw SIGINT no longer needs to be made available under the applicable MOA.

5. (U) *Access*. Limit access to raw SIGINT to those IC element personnel who have appropriate security clearances, accesses, training, and a mission need.

6. (U) *Auditing records*. Protect auditing records against unauthorized access, modification, or deletion, and retain these records for a sufficient period of time to verify compliance with the requirements of these Procedures.

7. (U) *Marking of files*. Use reasonable measures to identify and mark or tag raw SIGINT files reasonably believed or known to contain USPI. Marking and tagging will occur regardless of the format or location of the information, or the method of storing it. When appropriate and reasonably possible, files and documents containing USPI will also be marked individually. In the case of certain electronic databases, if it is not reasonably possible to mark individual files containing USPI, a banner may be used before access informing users that they may encounter USPI.

8. (U) *Disseminations*. Monitor disseminations of information derived from raw SIGINT to ensure compliance with the provisions of section VI below.

9. (U) *Removal of information*. Ensure that raw SIGINT is removed from all electronic and hard copy files within the time periods specified in section V below.

(U) SECTION IV – PROCESSING RAW SIGINT

A. (U) Intelligence purpose. An IC element obtaining raw SIGINT under these Procedures may only evaluate the raw information obtained for the authorized foreign intelligence or counterintelligence purposes documented in the applicable MOA.

B. (U) Selection of domestic communications prohibited. An IC element obtaining raw SIGINT under these Procedures may not use a query, identifier, or other selection term that is intended to select domestic communications.

C. (U) Selection terms based on identity. An IC element obtaining raw SIGINT under these Procedures may use a selection term that is intended to select foreign communications on the basis of the identity of a communicant or the fact that the communications mention a particular person. The IC element will take all reasonable measures, if necessary on an ongoing basis, to determine whether a selection term is associated with a U.S. person or a person in the United States and may not use such a term unless authorized in accordance with this paragraph. These measures may include appropriate coordination with NSA or other Government departments and agencies. The IC element may only intentionally select foreign communications of or concerning a U.S. person or a person in the United States if the element's compliance organization or legal counsel confirms that one of the following circumstances exists:

1. (U) *Current FISA targets*. Foreign communications known to be to, from, or about a U.S. person or a person located in the United States may be intentionally selected if such person is the subject of an order or emergency authorization authorizing electronic surveillance, a physical search, or an acquisition under sections 105, 304, 703, 704, or 705 of FISA, 50 U.S.C. §§ 1805, 1824, 1881c-e, at the time when such raw SIGINT is to be selected. (Note that this provision does not apply to a U.S. person or a person in the United States who is the subject of an order or emergency authorization under the pen register or business records provisions of FISA, 50 U.S.C. §§ 1842, 1843, 1861.) If there is any question about the applicability of such an order or authorization, the compliance organization or legal counsel must consult with the Office of Intelligence of the National Security Division, Department of Justice.

2. (U) *Other targets*. Unless authorized under paragraph 1, foreign communications reasonably likely to be to, from, or about a U.S. person or a person located in the United States may not be intentionally selected for the purpose of targeting a U.S. person or a person in the United States, unless approved by:

a. (U) The Attorney General, if all of the following requirements are met:

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

[redacted];

(ii) (U) The person is an agent of a foreign power or an officer or employee of a foreign power; and

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

(U) The Attorney General's approvals will be limited to a period of time not to exceed 90 days.

b. (U) The DIRNSA or the IC element head, or a high-level designee of the IC element head, if any of the following requirements is met:

(i) (U) The person consented, by completing an appropriate consent agreement, to the use by a recipient element of a selection term intended to select communications to, from, or about that person. The IC element will promptly provide NSA with a copy of all such approvals;

(ii) (U) The targeted individual is reasonably believed to be held captive by a foreign power or group engaged in international terrorism. When an IC element authorizes under this paragraph the selection of raw SIGINT concerning a U.S. person held captive, the IC element's legal counsel will, within 72 hours, notify the Attorney General and NSA's OGC, and in the case of a DoD IC element, will also notify DoD's OGC;

(iii) ~~(S//SI//REL)~~ [redacted];

(iv) ~~(S//SI//REL)~~ [redacted];

(v) ~~(S//SI//REL)~~ The targeted entity is a [redacted] business entity in the United States that is openly acknowledged to be directed or controlled by a foreign power. Any approval under this subparagraph will be granted as follows:

a. (U) If the DIRNSA is approving the selection, the DIRNSA will comply with the requirements of section 4.A.1(b) of the Classified Annex to Department of Defense Procedures Under E.O. 12333 or any successor documents.

b. (U) If an IC element head or a high-level designee is approving the selection, he or she will certify to the Attorney General that the targeted entity is openly acknowledged to be directed and controlled by a foreign power; that the purpose of the selection is to obtain foreign intelligence or counterintelligence information about that foreign power in accordance with valid intelligence requirements; and that the element will protect any USPI reviewed as a result of the selection in accordance with these Procedures. Such official will provide a copy of the certification to the DIRNSA or a designee, and will also advise the Attorney General and the DIRNSA on an annual basis of all such selections.

D. (U) Selection terms based on content. When a selection term is intended to select communications or related data on the basis of its content, rather than on the basis of the identity of the communicant or the fact that the communication mentions a particular person, the following rules apply:

1. ~~(S//SI//REL)~~ *Results anticipated from selection term*. No selection term that is reasonably likely to result in the retrieval of communications to or from a U.S. person (wherever located) [redacted], or data related to such communications, may be used unless there is reason to believe that foreign intelligence or counterintelligence will be obtained by the use of such selection term.

2. (U) *Results obtained from selection term*. No selection term that has resulted in the retrieval of a significant number of communications to or from such persons or entities, or data related to such communications, may be used unless there is reason to believe that foreign intelligence or counterintelligence will be obtained.

3. (U) *Minimize retrieval of communications that do not contain foreign intelligence or counterintelligence*. Selection terms that have resulted or are reasonably likely to result in the retrieval of communications to or from such persons or entities, or data related to such communications, will be designed to defeat, to the greatest extent practicable under the circumstances, the retrieval of those communications that do not contain foreign intelligence or counterintelligence.

E. (U) Attorney-client communications. An IC element receiving raw SIGINT will comply with any guidance promulgated by the Assistant Attorney General for National Security, after consultation with the ODNI, with respect to the processing, retention, and dissemination of attorney-client communications.

F. (U) Exception for communications metadata analysis. An IC element receiving raw SIGINT may conduct communications metadata analysis, including contact chaining, of the raw SIGINT only for valid, documented foreign intelligence or counterintelligence purposes. It may engage in these activities without regard to the location or nationality of the communicants. These activities are subject to all the requirements of these

Procedures, except for paragraphs B through E above, which do not apply to them. Each year by October 15th, any recipient IC element using the provisions of this paragraph will report to the Attorney General on (i) the kinds of information that the element is processing as communications metadata; (ii) the element's implementation of the protections required by these Procedures with respect to metadata; and (iii) any significant new legal or oversight issues that have arisen in connection with the element's processing or dissemination of communications metadata of U.S. persons. The element will provide a copy of this report to NSA's OGC, NSA's Civil Liberties and Privacy Office, the DNI's Civil Liberties Protection Officer, DoD's OGC, and the DoD Senior Intelligence Oversight Official (SIOO).

(U) SECTION V – RETENTION

A. (U) Time periods for retention of raw SIGINT. A recipient IC element may retain raw SIGINT for not more than five years after the information is first collected by NSA, unless the continued retention for up to an additional five years is approved in writing by the head of the recipient element as necessary to protect national security[1] and also approved by the DNI to the extent required under PPD-28 and any implementing policies. In no event, however, may a recipient element retain raw SIGINT beyond the time that NSA may retain it. A recipient IC element is responsible for ensuring compliance with applicable retention periods for any raw SIGINT transferred to its information systems. For any raw SIGINT that NSA provides to a recipient element, NSA must inform the recipient element of the applicable retention period.

B. (U) Foreign communications that have been minimized. Foreign communications to, from or about U.S. persons or data related to such communications may be permanently retained only:

1. (U) If processed so as to eliminate any USPI; or

2. (U) If dissemination of such communications without elimination of reference to such U.S. persons would be permitted under section VI below.

(U) Any retention must also be permitted under paragraphs D and E below.

C. (U) Domestic communications. Domestic communications inadvertently retrieved during the selection of foreign communications will be promptly destroyed upon recognition unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

[1] (U) Such approval must comply with section 309(b)(3)(B)(vii) of the 2015 Intelligence Authorization Act codified at 50 U.S.C. § 1813.

D. (U) Communications between U.S. persons. Communications solely between U.S. persons inadvertently retrieved during the selection of foreign communications will be destroyed upon recognition, except:

1. (U) When the communication contains significant foreign intelligence or counterintelligence, the head of the recipient IC element may waive the destruction requirement and subsequently notify the DIRNSA and NSA's OGC; or

2. (U) When the communication contains evidence of a crime or a threat of death or serious bodily harm to any person, or anomalies that reveal a potential vulnerability to U.S. communications security, the recipient IC element will notify NSA's OGC, which will review it according to the applicable NSA procedures and policies.

E. (U) Communications with government employees. Unless otherwise permitted by section IV, communications to or from any officer or employee of the U.S. Government or of any state, local, or tribal government, who are U.S. persons or located in the United States, will not be intentionally selected during the selection of foreign communications. Inadvertent retrieval of such communications solely between persons in the United States will be treated in accordance with paragraph C above. The inadvertent retrieval of any other communications to or from any officer or employee of the U.S. Government or of any state, local, or tribal government (including those between foreign targets and U.S. officials) will be treated in accordance with paragraph D above.

F. (U) Immediate notice required. When a recipient IC element identifies a communication requiring destruction under paragraph C, D, or E, the element will notify the DIRNSA's designee and NSA's OGC immediately upon recognition.

(U) SECTION VI - DISSEMINATION

A. (U) Consistency with other requirements

1. (U) *Other laws*. All disseminations under these Procedures must be permissible under the Privacy Act, 5 U.S.C. § 552a, if applicable, and other laws.

2. (U) *Memorandum of agreement*. All disseminations under these Procedures must be permissible under IC policy and the MOA concluded between NSA and the recipient IC element under paragraph II.D.1.

B. (U) Criteria for dissemination of USPI. Subject to paragraph A and to paragraphs C, D, and E below, an IC element may disseminate USPI derived solely from raw SIGINT covered by these Procedures only if one of the following conditions is met, and

if a high-level official as specified in the MOA determines that the recipient has a need for the USPI in the performance of his or her official duties:

1. (U) *Consent*. The U.S. person has consented to the dissemination of (i) communications to, from, or about him or her, (ii) data related to such communications, or (iii) information about him or her, and has executed an appropriate consent form.

2. (U) *Publicly available*. The USPI is publicly available information.

3. (U) *Understanding foreign intelligence or counterintelligence*. The USPI is necessary to understand the foreign intelligence or counterintelligence information or assess its importance. The following nonexclusive list contains examples of the type of information that meets this standard:

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

b. (U) The information indicates that the U.S. person may be engaged in the unauthorized disclosure of classified information;

c. (U) The information indicates that the U.S. person may be engaged in international narcotics trafficking activities;

d. (U) The information indicates that the U.S. person may be the target of hostile intelligence activities of a foreign power;

e. (U) The information is 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

f. (U) The identity is that of a senior official of the Executive Branch of the U.S. Government. In this case, normally only the official's title will be disseminated. A high-level official of the recipient IC element will ensure that domestic political or personal information that is not necessary to understand foreign intelligence or counterintelligence or assess its importance is not retained or disseminated.

4. (U) *Evidence of a crime*. The information is evidence of a possible commission of a crime and reported as provided in the Memorandum of Understanding: Reporting of Information Concerning Federal Crimes, or any successor documents.

5. (U) *Required disseminations*. The dissemination is required by statute; treaty; executive order; Presidential directive; National Security Council directive; Homeland Security Council directive; or policy, memorandum of understanding, or agreement approved by the Attorney General.

C. (U) Disseminations to foreign governments or government-sponsored international entities. In addition to the other requirements of this section, the DIRNSA or a designee (who may be an official of another IC element) must approve any disseminations of information obtained under these procedures to a foreign government or a government-sponsored international entity. The approving official must determine that the disclosure is consistent with applicable international agreements and foreign disclosure policy and directives, including those requiring analysis of potential harm to any individual.

D. (U) Dissemination of raw SIGINT prohibited. An IC element receiving raw SIGINT under these Procedures may not further disseminate the raw SIGINT it obtains. If a recipient IC element wishes to disseminate raw SIGINT, it must request authorization from the DIRNSA. The DIRNSA or a high-level designee may authorize the dissemination if he or she finds, after consulting with NSA's General Counsel, that the dissemination is permissible under the procedures applicable to NSA.

E. (U) Other disseminations. NSA's OGC, in consultation with the National Security Division of the Department of Justice and DoD's OGC, must approve any dissemination that does not conform to the requirements of these Procedures. Such approval will be based on a determination that the proposed dissemination complies with applicable law, executive orders, and Presidential and IC directives.

(U) SECTION VII - TRAINING, AUDITING, AND OVERSIGHT

A. (U) Training. All IC element personnel who have access to raw SIGINT under these Procedures will receive training on these Procedures. IC elements will develop this training in coordination with NSA, and pursuant to training standards developed by ODNI in consultation with DoD. The training will include, if applicable, the avoidance of selection terms associated with U.S. persons or a person in the United States; the use of selection terms based on content; the need to consult with a supervisor about selection terms whose use may not be appropriate because of the communications to, from, or about U.S. persons likely to be retrieved; other processing, retention, and dissemination requirements; and the proper use and dissemination of metadata in accordance with paragraph IV.F.

B. (U) Auditing. An IC element obtaining access to raw SIGINT must have auditing capabilities and requirements that are comparable to NSA's and meet the following minimum standards:

1. (U) *Access*. Access to raw SIGINT will be monitored, recorded, and audited by supervisory or other appropriate personnel;

2. (U) *Queries*. All queries or other search terms will be monitored and recorded, and supervisory or other appropriate personnel will audit and review the use of such terms. The recipient IC element's compliance program will specify the periodicity of the audits which, at a minimum, will be comparable to NSA's. The results of the audits will be provided to the officials conducting reviews under section VII.G; and

3. (U) *Retrievals*. Retrievals, or samples of retrievals, from repositories of raw SIGINT will be reviewed for compliance with these Procedures and for their relevance to the authorized mission or function for which access has been provided.

C. (U) IC element oversight and compliance programs. Each IC element, in coordination with the IC element's legal, oversight, compliance, and privacy and civil liberties officials (and the DoD SIOO in the case of a DoD IC element), will establish an oversight and compliance program for handling raw SIGINT provided under these Procedures. The IC element's oversight and compliance program will be reviewed and approved by the DNI's Civil Liberties Protection Officer, in consultation with NSA, to ensure that the program is comparable to NSA's for similar activities. This program will:

1. (U) Implement the training and auditing required by subsections A and B;

2. (U) Ensure that the element uses selection terms and processes raw SIGINT, including metadata, in accordance with section IV;

3. (U) Ensure that the element does not improperly retain and/or disseminate USPI; and

4. (U) Include oversight and compliance measures comparable to those used by NSA in similar circumstances.

D. (U) Assistance to recipient IC elements. NSA will assist recipient IC elements in establishing oversight and compliance programs to meet the requirements of these Procedures. NSA will also make available training material required for, and prior to, access to raw SIGINT.

E. (U) Questionable intelligence activities. An IC element will report in writing to the DIRNSA's designee (and, in the case of DoD IC elements, to the DoD SIOO) any questionable intelligence activity (including compliance incidents or other violations of these Procedures) by IC element personnel concerning raw SIGINT obtained under these Procedures. Such reporting will be completed immediately upon recognition. The report will also be included in the IC element's normal intelligence oversight reporting to, among others, the President's Intelligence Oversight Board and the ODNI.

F. (U) Other reporting responsibilities. These Procedures do not supersede or replace reporting responsibilities required by law, executive order, directive, regulation, policy, or other guidance, including E.O. 13462.

G. (U) Reviews

1. (U) *Reviews by the IC element and ODNI*. Appropriate oversight, compliance, and privacy and civil liberties officials of an IC element receiving raw SIGINT, in coordination with the DNI's Civil Liberties Protection Officer (and the DoD SIOO in the case of a DoD IC element), will in accordance with the applicable MOA periodically, but not less than every three years, evaluate practices for protecting USPI, the adequacy of the oversight and compliance activities conducted in accordance with these Procedures, and the adequacy and timeliness of the reporting required by these Procedures. The IC element will promptly correct any deficiencies identified. The DNI's Civil Liberties Protection Officer will report major deficiencies to the head of the IC element, the DIRNSA, and the DNI.

2. (U) *ODNI assessment of overall IC implementation of these Procedures*. Based on the reviews jointly conducted by IC elements and ODNI in paragraph 1 above and the reporting of questionable intelligence activities, the DNI's Civil Liberties Protection Officer will periodically, but not less than every three years, review how the IC is implementing these Procedures, the gravity of any compliance incidents across the IC, and the frequency, trends, or patterns of the incidents across the IC to assess whether programmatic adjustments to the way these Procedures are implemented are warranted, or whether any additional action is needed. The DNI's Civil Liberties Protection Officer will report major deficiencies to the DNI, the Secretary of Defense, and the DIRNSA.

3. (U) *NSA's authority to review*. Nothing in these Procedures is intended to preclude NSA, in accordance with the responsibilities of its Director under sections 1.3(b)(12)(A)(i) and 1.7(c) of E.O. 12333, from reviewing a recipient IC element's handling of raw SIGINT made available under these Procedures. Recipient IC elements must comply with NSA's requests for information in support of any such review. If NSA determines that an IC element has failed to comply with the requirements of E.O. 12333 or these Procedures, DIRNSA's designee may terminate the IC element's access to raw SIGINT without notice.

(U) SECTION VIII - USE IN LEGAL PROCEEDINGS

(U) A recipient IC element may not use, or permit the use of, raw SIGINT made available under these Procedures, or information derived from such information, in any legal or administrative proceeding without the prior approval of NSA's OGC.

(U) SECTION IX - GENERAL PROVISIONS

A. (U) Correspondence. The DIRNSA, or a designee, will be included as an addressee on all significant official correspondence on matters pursuant to these Procedures.

B. (U) Delegation. When these Procedures require a specific official to approve an activity or take some other action, only that official, or an official at a higher level in the chain of command, may take that action. When these Procedures permit an official to delegate responsibility for an action, the official may delegate the responsibility to one or more appropriate officials in accordance with IC element or department policy, unless specifically limited to a single designee.

C. (U) Interpretation. NSA will refer all questions relating to the interpretation of these Procedures to NSA's OGC. NSA's OGC will consult with the Assistant Attorney General for National Security, ODNI's OGC, and DoD's OGC regarding any novel or significant interpretations of these Procedures. IC elements receiving raw SIGINT under these Procedures will refer all questions relating to the interpretation of these Procedures to the appropriate legal office in the IC element (and, in the case of DoD IC elements, also to DoD OGC). The appropriate legal office will consult with the Assistant Attorney General for National Security and the ODNI, NSA, and DoD OGCs regarding any novel or significant interpretations of these Procedures. NSA's Civil Liberties and Privacy Office, the DNI's Civil Liberties Protection Officer, and DoD's Privacy and Civil Liberties Office will be informed of any novel or significant interpretation of these Procedures.

D. (U) Departures. The ODNI General Counsel and the Assistant Attorney General for National Security, after consultation with NSA's General Counsel, must approve any departures from these Procedures. If there is insufficient time for such approval because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, the head of an IC element or the head's senior representative present may approve a departure from these Procedures. The General Counsel of NSA will be notified as soon thereafter as possible. The IC element will provide prompt written notice of any such departures to the General Counsel of NSA, the Assistant Attorney General for National Security, the ODNI General Counsel, and to the DoD General Counsel. The NSA General Counsel will notify the DoD General Counsel and the Assistant Attorney General for National Security of any such departures that are not otherwise reported. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

E. (U) Internal Guidance. These Procedures are set forth solely for the purpose of internal U.S. Government guidance. They are not intended to, do 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 do they place any limitation on otherwise lawful investigative and litigative prerogatives of the United States.

F. (U) Review of these Procedures. The DNI will complete a review of these Procedures and their implementation within five years after they are established. This review will consider the implementation of these Procedures from both the information sharing and the civil liberties and privacy perspectives. The DNI will conduct this review in coordination with the Attorney General and Secretary of Defense and will consider whether any findings from the review warrant amendments to these Procedures.

(U) SECTION X - DEFINITIONS

A. (U) Agent of a foreign power means:

1. (U) Any person, other than a U.S. person, who:

   a. (U) Acts in the United States as an officer or employee of a foreign power, or as a member of a group engaged in international terrorism or activities in preparation therefor, irrespective of whether the person is in the United States;

   b. (U) 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. (U) Engages in international terrorism or activities in preparation therefor;

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

   e. (U) 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. (U) Any person, including a U.S. person, who:

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

d. (U) Knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

e. (U) Knowingly aids or abets any person in the conduct of activities described in paragraphs a through c or knowingly conspires with any person to engage in those activities.

B. (U) Communicant means a sender or intended recipient of a communication.

C. (U) Communications about a U.S. person are those in which the U.S. person is identified in the communication. A U.S. person is identified when the person's name, unique title, address, or other USPI is revealed in the communication in the context of activities conducted by that person or activities conducted by others and related to that person. A mere reference to a product by brand name or manufacturer's name, *e.g.*, "Boeing 707" is not an identification of a U.S. person.

D. (U) Communications metadata means the dialing, routing, addressing, or signaling information associated with a communication, but does not include information concerning the substance, purport, or meaning of the communication. The two principal subsets of communications metadata are telephony metadata and electronic communications metadata:

1. (U) Telephony "metadata" includes the telephone number of the calling party, the telephone number of the called party, and the date, time, and duration of the call. It does not include the substance, purport, or meaning of the communication.

2. (U) For electronic communications, "metadata" includes 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, and the "to," "cc," and "bcc" lines contain the e-mail addresses of the recipients. "Metadata" also means (i) information about the Internet-protocol (IP) address of the computer from which an e-mail or other electronic communication was sent and, depending on the circumstances, the IP address of routers and servers on the Internet that have handled the communication during transmission; (ii) the exchange of an IP address and e-mail

address that occurs when a user logs in to a web-based e-mail service; and (iii) for certain logins to web-based e-mail accounts, inbox metadata that is transmitted to the user upon accessing the account. "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.

E. (U) Contact chaining is 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.

F. (U) Counterintelligence means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

G. (U) Dissemination means the transmission, communication, sharing, or passing of information outside an IC element by any means, including oral, electronic, or physical means. Dissemination therefore includes providing any access to information in an IC element's custody to persons outside that IC element.

H. (U) Domestic communication means any communication where the sender and all intended recipients are located in the United States and that was acquired under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

I. (U) Foreign communication means a communication that involves a sender or an intended recipient who is outside the United States.

J. (U) Foreign intelligence means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons or international terrorists.

K. (U) Foreign power means any of the following:

1. (U) A foreign government or any component thereof, whether or not recognized by the United States.

2. (U) A faction of a foreign nation or nations, not substantially composed of U.S. persons.

3. (U) An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.

4. (U) A group engaged in international terrorism or activities in preparation therefor.

5. (U) A foreign-based political organization, not substantially composed of U.S. persons.

6. (U) An entity that is directed and controlled by a foreign government or governments.

7. (U) An entity not substantially composed of U.S. persons that is engaged in international proliferation of weapons of mass destruction.

L. (U) IC element is as defined in section 3.5(h) of E.O. 12333.

M. (U) International terrorism means activities that (i) involve violent acts or acts dangerous to human life that violate federal, State, local, or tribal criminal law or would violate such law if committed in the United States or a state, local, or tribal jurisdiction; (ii) appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by assassination or kidnapping; and (iii) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

N. (U) Publicly available information means information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public.

O. (U) Questionable intelligence activity means an intelligence activity that may violate the law, E.O. 12333, any other executive order or Presidential directive, or applicable policy of the IC element, including these Procedures.

P. (U) Raw SIGINT is any SIGINT and associated data that has not been evaluated for foreign intelligence purposes and/or minimized.

Q. (U) Selection, as applied to manual and electronic processing activities, means the intentional insertion of a name, cable address, telex number or answer back, address, telephone number, email address, or other alphanumeric device or identifier into a

computer scan dictionary or manual scan guide for the purpose of identifying messages or information of interest and isolating them for further processing.

R. (U) Selection term means the composite of individual terms used to effect or defeat selection of particular communications or information. It comprises the entire term or series of terms so used, but not any segregable term contained therein. It applies to both electronic and manual processing.

S. (U) Unevaluated SIGINT is SIGINT that has not been evaluated to determine whether it contains foreign intelligence or counterintelligence information.

T. (U) United States. When used in a geographic sense, means the land area, internal waters, territorial seas, and airspace of the United States, including U.S. territories, possessions, and commonwealths.

U. (U) Unminimized SIGINT is SIGINT that has not been reviewed to delete or mask USPI not meeting the standards for permanent retention and dissemination under the Classified Annex to Department of Defense Procedures Under E.O. 12333, these Procedures, or other procedures approved by the Attorney General.

V. (U) U.S. person. The term "U.S. person" means any of the following:

1. (U) A U.S. citizen;

2. (U) An alien known by the IC element concerned to be a permanent resident alien.

3. (U) An unincorporated association substantially composed of U.S. citizens or permanent resident aliens.

4. (U) A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a U.S. person.

(U) In applying paragraph 3, if a group or organization in the United States that is affiliated with a foreign-based international organization operates directly under the control of the international organization and has no independent program or activities in the United States, the membership of the entire international organization shall be considered in determining whether it is substantially composed of U.S. persons. If, however, the U.S.-based group or organization has programs or activities separate from, or in addition to, those directed by the international organization, only its membership in the United States will be considered in determining whether it is substantially composed of U.S. persons.

(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. Conversely, a person or entity 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.

W. (U) U.S. person information (USPI). USPI is information that is reasonably likely to identify one or more specific U.S. persons. USPI may be either a single item of information or information that, when combined with other information, is reasonably likely to identify one or more specific U.S. persons. Determining whether information is reasonably likely to identify one or more specific U.S. persons in a particular context may require a case-by-case assessment by a trained intelligence professional. It is not limited to any single category of information or technology.

(U) Depending on the context, examples of USPI may include names or unique titles; government-associated personal or corporate identification numbers; unique biometric records; financial information; and street address, telephone, and Internet Protocol address information.

(U) USPI does not include:

A reference to a product by brand or manufacturer's name or the use of a name in a descriptive sense, as, for example, "Ford Mustang" or "Boeing 737;" or

Imagery from overhead reconnaissance or information about conveyances (*e.g.*, vehicles, aircraft, or vessels) without linkage to additional identifying information that ties the information to a specific U.S. person.

(U) I establish the foregoing Raw SIGINT Availability Procedures in accordance with section 2.3 of E.O. 12333.

James R. Clapper
Director of National Intelligence

15 Dec 2016
Date

APPROVED:

Loretta E. Lynch
Attorney General

3 January 2017
Date