Annex A to Policy 12-3/
Annotated DoDM 5240.01 15 February 2022

The content of DoDM 5240.01 is included below in its entirety with the exception that ALL references to Defense Intelligence Components or the Component's pertinent organization (e.g., legal, civil liberties and privacy) have been changed to NSA/CSS or the appropriate NSA/CSS organization.

DoD Manual 5240.01

(U) Procedures Governing the Conduct of DoD Intelligence Activities

Originating Component:	Office of the Deputy Chief Management Officer of the Department of Defense
Effective:	August 8, 2016
Releasability:	Cleared for public release. Available on the DoD Issuances Website at http://www.dtic.mil/whs/directives.
Incorporates and Cancels:	Directive-type Memorandum 08-011, "Intelligence Oversight Policy Guidance," March 26, 2008 Procedures 1-10 of DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 7, 1982
Approved by:	Loretta B. Lynch, Attorney General of the United States Ashton B. Carter, Secretary of Defense

Purpose: In accordance with the authority in DoD Directive 5240.01 and Executive Order (E.O.) 12333, this issuance:

- Establishes procedures to enable DoD to conduct authorized intelligence activities in a manner that protects the constitutional and legal rights and the privacy and civil liberties of U.S. persons. DoD authorized intelligence activities are foreign intelligence and counterintelligence (CI) activities unless otherwise specified in this issuance.

- Authorizes the Defense Intelligence Components to collect, retain, and disseminate information concerning U.S. persons in compliance with applicable laws, Executive orders, policies, and regulations.

TABLE OF CONTENTS

The content of DoDM 5240.01 is included below in its entirety with the exception that ALL references to Defense Intelligence Components or the Component's pertinent organization (e.g., legal, civil liberties and privacy) have been changed to NSA/CSS or the appropriate NSA/CSS organization.

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies including the National Security Agency (NSA)/Central Security Service (CSS), the DoD Field Activities, and all other organizational entities within the DoD, including elements of the Reserve Components and the National Guard, or anyone acting on behalf of those components or elements, when conducting intelligence activities under DoD's authorities (referred to collectively in this issuance as the "DoD Components"). Coast Guard service members who are detailed to and assigned duties supervised by DoD Intelligence Components and are conducting DoD intelligence activity are subject to this Manual. When, pursuant to Presidential or Congressional action, the Coast Guard operates as a service in the Navy, the provisions of this Manual will apply to all Coast Guard Intelligence activity.

1.2. POLICY. In accordance with the authority in DoD Directive 5240.01 and E.O. 12333, it is DoD policy that:

a. All Defense intelligence activities will be conducted in accordance with applicable laws, Executive orders, and Presidential directives, and governed by procedures issued by the Secretary of Defense and, where appropriate, approved by the Attorney General in accordance with E.O. 12333.

b. In carrying out intelligence activities, NSA/CSS:

(1) Is authorized to collect, retain, and disseminate information concerning U.S. persons and conduct other activities only in accordance with the procedures in this issuance.

(2) Must carry out all activities in all circumstances in accordance with the Constitution and laws of the United States.

(3) May not investigate U.S. persons or collect or maintain information about them solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States.

(4) Will not participate in or request any person or entity to undertake any activities that are forbidden by E.O. 12333 or this issuance.

1.3. PROCEDURES. a. The procedures in Section 3 and the definitions in the Glossary, which implement the provisions of E.O. 12333, have been approved by the Attorney General after consultation with the Director of National Intelligence.

b. Procedures 11 through 15 of DoD 5240.1-R will remain in effect until incorporated and cancelled by other DoD guidance. The classified annex of DoD 5240.1-R will remain in effect until superseded.

1.4. INTERNAL GUIDANCE. This manual is published solely for internal DoD 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.

1.5 INFORMATION COLLECTIONS. 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 OMB Control Number in accordance with Paragraph 8.a.(2)(d) of Enclosure 3 of Volume 2 of DoD Manual 8910.01.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)). The USD(I&S) approves all intelligence activities that the Secretary of Defense may approve in accordance with this issuance, except where specifically limited by statute, Executive order, or DoD policy.

2.2. DOD COMPONENT HEADS. DIRNSA/CHCSS may issue implementing instructions for the conduct of authorized missions or functions consistent with the procedures in this issuance.. In developing such instructions, DIRNSA/CHCSS should consult with NSA/CSS privacy and civil liberties official, the NSA/CSS CLPT (D5).

SECTION 3: PROCEDURES

3.1. PROCEDURE 1. GENERAL PROVISIONS. a. Scope. (1) NSA/CSS provides necessary information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents. The procedures in this issuance govern the conduct of NSA/CSS and non-intelligence components or elements, or anyone acting on behalf of those components or elements, when conducting intelligence activities under DoD's authorities.

(2) Procedure 1 establishes the scope and administrative provisions for implementing this issuance. Procedures 2 through 4 articulate the procedures through which NSA/CSS and those personnel within the scope of Paragraph 3.1.a.(1) are authorized to collect, retain, and disseminate U.S. person information (USPI). Procedures 5 through 10 govern the use of certain collection techniques to obtain information for foreign intelligence and CI purposes. The classified or SIGINT annex to this issuance supplements Procedure 5. NSA/CSS will employ the techniques governed by Procedures 5 through 10 only as necessary to perform missions or functions assigned to the Component. Procedures 6-9, however, cover techniques not authorized for NSA/CSS to use.

(3) Activities not governed by this issuance will be carried out in accordance with other applicable policies and procedures, including Presidential directives that govern those particular missions or functions. When specifically authorized by the Secretary of Defense or delegee to perform missions or functions other than foreign intelligence or CI, NSA/CSS will comply with DoD policy applicable to DoD non-intelligence organizations and any specific operational parameters specified by the Secretary of Defense for that mission or function. Examples of such activities are:

(a) Law enforcement or civil disturbance activities conducted under DoD authorities or activities of individuals executing a law enforcement, physical security, or force protection mission.

(b) Defense support of civil authorities, when directed by the Secretary of Defense. Defense support of civil authorities activities is conducted consistent with the National Response Framework, and includes the provision of humanitarian assistance; disaster readiness, response, and recovery activities; and environmental and security vulnerability studies.

(c) Activities conducted pursuant to Section 442 of Title 10, United States Code (U.S.C.) or Section 3045 of Title 50, U.S.C. for humanitarian assistance; disaster readiness, response, and recovery; maritime and aeronautical safety of navigation; environmental and security vulnerability studies; mapping, charting, and geodetic missions; and other similar activities not constituting foreign intelligence or CI and authorized pursuant to Section 442 of Title 10, U.S.C. or Section 3045(b) of Title 50, U.S.C.

(d) Activities fulfilling the responsibilities of the National Manager for National Security Systems.

(4) NSA/CSS is not authorized to and will not engage in any intelligence activity, including dissemination to the White House, for the purpose of affecting the political process in

the United States. Additional guidance regarding the application of this prohibition will be issued by the DoD Senior Intelligence Oversight Official (SIOO) after consultation with the Director of National Intelligence. Questions about whether a particular activity falls within this prohibition will be resolved in consultation with the NSA OGC and the General Counsel of the Department of Defense (GC DoD).

(5) NSA/CSS will report a possible violation of federal criminal law by an employee or a possible violation of specified federal criminal laws by any other person, as required by Section 1.6(b) of E.O. 12333, in accordance with the August 22, 1995 DoD and Department of Justice Memorandum of Understanding on Reporting of Information Concerning Federal Crimes.

(6) When this issuance requires a specific DoD 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 this issuance permits an official to delegate authority for an action, the official may delegate the authority to one or more appropriate officials in accordance with DoD policy, unless specifically limited to a single delegee.

b. Shared Repositories.

(1) General. NSA/CSS may host or participate in a shared repository containing USPI only in accordance with this issuance and applicable laws and policies.

(2) NSA/CSS Acting as Host. NSA/CSS acting as a host of a shared repository may perform systems support functions or data-related tasks (e.g., tagging, processing, or marking information) for itself or others. Access to USPI solely for these purposes does not constitute collection, retention, or dissemination pursuant to this issuance. NSA/CSS must enable audit of access to USPI in a shared repository to the extent practicable. Each participant in a shared repository must inform NSA/CSS in writing that its participation complies with all law, policies, and procedures applicable to the protection of USPI.

(3) NSA/CSS Acting as a Participant. NSA/CSS acting as a participant in a shared repository must ensure that its access to and use of the repository complies with law, policies, and procedures applicable to protection of USPI (including this issuance), and must identify to the host any access and use limitations applicable to the USPI it provides. A participating Component that provides USPI to a shared repository and allows access to or use of USPI by other participants has made a dissemination, and may do so only in accordance with Procedure 4 or other applicable Attorney General-approved guidelines. This does not include access to or use of USPI by a host or another element of the Intelligence Community for systems support functions or data-related tasks.

c. Interpretation. The procedures in this issuance will be interpreted in accordance with their stated purpose. All questions of interpretation will be referred to the NSA OGC, "Go GC" or DL D2_Action. Questions that cannot be resolved in this manner will be referred to the NSA General Counsel or, as appropriate, to the GC DoD or the DoD SIOO for resolution. As appropriate, privacy and civil liberties officials will be consulted. The GC DoD will consult with

the Assistant Attorney General for National Security regarding any novel or significant interpretations of this issuance and the potential applicability of Intelligence Community Directive 102.

d. Exceptions to Policy. NSA/CSS may submit written requests for exceptions to policy in this issuance through the NSA OGC to the DoD SIOO. In considering making requests for exceptions to policy, NSA/CSS should consult with the NSA/CSS CLPT.

(1) The DoD SIOO will present all requests for exceptions to policy to the Secretary of Defense after consultation with the GC DoD. Exceptions to policy require the approval of the Assistant Attorney General for National Security.

(2) If time requirements constrain such review and approval, and an exception to these Procedures is necessary due to the immediacy or gravity of a threat to the safety of persons, DoD property, or the national security, DIRNSA/CHCSS or the Component's senior representative present (e.g., DDIR, EXDIR, SOO, NCR) may approve an exception to these Procedures. The GC DoD and DoD SIOO will be notified as soon thereafter as possible and the GC DoD will provide prompt written notice of any such exceptions to the Assistant Attorney General for National Security. All activities in all circumstances must be carried out in accordance with the Constitution and laws of the United States.

e. Amendments. NSA/CSS may submit written requests for amendment to this issuance through the NSA OGC to the DoD SIOO. In considering making requests for amendments, NSA/CSS should consult with their respective privacy and civil liberties officials. The DoD SIOO will present all requests for amendments to the Secretary of Defense after consultation with the GC DoD. Amendments require the approval of the Attorney General after consultation with the Director of National Intelligence.

3.2. PROCEDURE 2. COLLECTION OF USPI.

a. Scope. This procedure specifies the general criteria governing the collection of USPI. Only Paragraphs 3.2.f. and 3.2.g. apply to the acquisition of information in accordance with Chapter 36 of Title 50, U.S.C., also known and referred to in this issuance as "the Foreign Intelligence Surveillance Act (FISA)."

b. Definition of Terms. See the Glossary for definitions of "administrative purposes," "CI," "collection," "consent," "cooperating sources," "domestic activities," "foreign connection," "foreign intelligence," "foreign power," "host of a shared repository," "incidental collection of USPI," "intentional collection of USPI," "international narcotics activities," "overhead reconnaissance," "publicly available," "reasonable belief," "shared repository," "U.S. person," and "USPI."

c. Intentional Collection of USPI. NSA/CSS may intentionally collect USPI only if the information sought is reasonably believed to be necessary for the performance of an authorized

intelligence mission or function assigned to the Component, and if the USPI falls within one of the following categories:

(1) Publicly Available. The information is publicly available.

(2) Consent. The information concerns a U.S. person who has consented to such collection.

(3) Foreign Intelligence. The information is reasonably believed to constitute foreign intelligence and the U.S. person is:

(a) An individual reasonably believed to be an officer or employee of, or otherwise acting on behalf of, a foreign power;

(b) An organization or group reasonably believed to be directly or indirectly owned or controlled by, or acting on behalf of, a foreign power;

(c) An individual, organization, or group reasonably believed to be engaged in or preparing to engage in international terrorist or international narcotics activities;

(d) A corporation or other commercial organization reasonably believed to have some relationship with a foreign power, organization, or person; or

(e) An individual reasonably believed to be a prisoner of war or missing in action; or

(f) An individual, organization, or group who is a target, hostage, or victim of an international terrorist or international narcotics organization.

(4) CI. The information is reasonably believed to constitute CI and the U.S. person is one of the following:

(a) An individual, organization, or group reasonably believed to be engaged in or preparing to engage in espionage, other intelligence activities, sabotage, or assassination on behalf of a foreign power, organization, or person, or on behalf of an agent of a foreign power;

(b) An individual, organization, or group reasonably believed to be engaged in or preparing to engage in international terrorist activities;

(c) An individual, organization, or group reasonably believed to be acting for, or in furtherance of, the goals or objectives of an international terrorist or international terrorist organization, for purposes harmful to the national security of the United States; or

(d) An individual, organization, or group in contact with a person described in Paragraphs 3.2.c.(4)(a) through (c) for the purpose of identifying such individual, organization, or group and assessing any relationship with the person described therein.

(5) Threats to Safety. The information is needed to protect the safety of any person or organization, including those who are targets, victims, or hostages of international terrorist organizations. NSA/CSS will only collect information that is needed to protect the safety of any person or organization if:

(a) The threat has a foreign connection;

(b) DIRNSA/CHCSS or a delegee has determined that a person's life or physical safety is reasonably believed to be in imminent danger; or

(c) The information is needed to maintain maritime or aeronautical safety of navigation.

(6) Protection of Intelligence Sources, Methods, and Activities. The information is about U.S. persons who have access to, had access to, will have access to, or are otherwise in possession of information that reveals foreign intelligence or CI sources, methods, or activities, when collection is reasonably believed necessary to protect against the unauthorized disclosure of such information. Within the United States, NSA/CSS will limit intentional collection of such information to persons who are:

(a) Current or former DoD employees;

(b) Current or former employees of current or former DoD contractors; or

(c) Applicants seeking employment with the DoD or a DoD contractor.

(7) Current, Former, or Potential Sources of Assistance to Intelligence Activities. The information is about those who are or have been sources of information or assistance, or are reasonably believed to be potential sources of information or assistance, to intelligence activities for the purpose of assessing their suitability or credibility. This category does not include investigations undertaken for personnel security purposes.

(8) Persons in Contact With Sources or Potential Sources. The information is about persons in contact with sources or potential sources, for the purpose of assessing the suitability or credibility of such sources or potential sources.

(9) Personnel Security. The information is arising from a lawful personnel security investigation.

(10) Physical Security. The information is about U.S. persons reasonably believed to have a foreign connection and who pose a threat to the physical security of DoD personnel, installations, operations, or visitors. NSA/CSS may also collect such information in the course of a lawful investigation resulting from a physical security inspection, vulnerability assessment, or reported security incident. In all cases, the collecting Component must have or be supporting an authorized physical security mission and must be able to articulate a reasonable belief in both the

foreign connection of the U.S. persons who are collection targets and the physical security threat they pose.

(11) Communications Security Investigation. The information is arising from a lawful communications security investigation.

(12) Overhead and Airborne Reconnaissance. The information is obtained from overhead and airborne reconnaissance, including from unmanned aircraft systems and imagery from overhead or airborne collection platforms operated commercially or obtained from other sources.

(a) A Defense Intelligence Component may intentionally collect imagery that contains USPI provided that the collection is not directed at a specific U.S. person or, if the collection is directed at a specific U.S. person, the collection falls in one of the other categories authorized by Paragraph 3.2.c.

(b) Collection of any domestic imagery must also comply with other applicable laws, policies, and procedures, including DoD or National Geospatial-Intelligence Agency (NGA) policies and procedures that govern such collection.

(c) All collection of imagery must comply with constitutional and statutory requirements, Executive orders, and Presidential directives, and the other provisions of this issuance.

(13) Administrative Purposes. The information is required for administrative purposes.

d. Incidentally Collected or Voluntarily Provided USPI. In the course of authorized collection activities, NSA/CSS may incidentally collect USPI. Entities or individuals may also on their own initiative voluntarily provide information to NSA/CSS. All such information may be temporarily retained, evaluated for permanent retention, and disseminated only in accordance with Procedures 3 and 4. If an entity or individual is voluntarily providing on a recurring basis USPI that is not relevant to an authorized mission or function assigned to NSA/CSS, then NSA/CSS will take appropriate steps to address such collection.

e. Special Circumstances Collection. NSA/CSS will consider whether collection opportunities raise special circumstances based on the volume, proportion, and sensitivity of the USPI likely to be acquired, and the intrusiveness of the methods used to collect the information. When special circumstances exist, DIRNSA/CHCSS or a delegee must determine whether to authorize the collection and, if so, whether enhanced safeguards are appropriate. If advance authorization is not possible, then as soon as possible after collection, DIRNSA/CHCSS or a delegee must authorize the continued temporary retention of the information in accordance with Paragraphs 3.2.e.(1) and (2) and Procedure 3. The approving official will provide notice of the approval to the DoD SIOO. After consulting with NSA's Office of the General Counsel and the NSA/CSS Civil Liberties, Privacy, and Transparency Office (D5), NSA/CSS will issue guidance on the implementation of this provision in accordance with Paragraph 2.2. In addition, any question about whether special circumstances exist will be resolved in consultation with NSA

OGC (D2) and CLPT (D5). An authorization of special circumstances collection will be based on both of the following:

(1) The information will be or has been properly collected in accordance with Paragraph 3.2.c and the other provisions of this procedure; and

(2) The collection activity is reasonable based on all the circumstances, including the value of the information; the collection methods used by NSA/CSS or others; the amount of USPI; the nature and sensitivity of the USPI; the civil liberties and privacy implications of the collection; the potential for substantial harm, embarrassment, inconvenience, or unfairness to U.S. persons if the USPI is improperly used or disclosed; and the safeguards that will be applied to the collected information in accordance with Paragraph 3.3.g.

f. General Criteria Governing the Means Used to Collect USPI.

(1) Means of Collection.NSA/CSS is authorized to collect USPI by any lawful means, provided that all such collection activities are carried out in accordance with E.O. 12333 and this issuance.

(2) Restriction on Purpose.NSA/CSS may not collect USPI solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States.

(3) Least Intrusive Means.NSA/CSS will use the least intrusive collection techniques feasible within the United States or directed against a U.S. person abroad. In general, this means:

(a) To the extent feasible, such information will be collected from publicly available sources or with the consent of the person concerned.

(b) If collection from publicly available sources or obtaining consent from the person concerned is not feasible or sufficient, such information may be collected from cooperating sources.

(c) If collection from cooperating sources is not feasible or sufficient, such information may be collected using other lawful intelligence collection techniques that do not require a judicial warrant or the approval of the Attorney General.

(d) If collection in accordance with Paragraphs 3.2.f.(3) (a) through (c) is not feasible or sufficient, approval may be sought through the GC DoD for the use of intelligence collection techniques that require a judicial warrant or approval from the Attorney General.

(4) Amount of Information Collected.Subject to Paragraph 3.2.f.(3), in collecting non-publicly available USPI, NSA/CSS will, to the extent practicable, collect no more information than is reasonably necessary.

g. Limitations on the Collection of Foreign Intelligence in the United States. NSA/CSS may only collect foreign intelligence concerning U.S. persons in the United States if:

(1) The information is publicly available;

(2) The source of the information is advised or is otherwise aware that he or she is providing information to DoD or a Defense Intelligence Component; or

(3) NSA/CSS employs other sources or methods of collection in or directed at the United States and all of the following conditions are met:

(a) The foreign intelligence sought is significant and collection is not undertaken for the purpose of acquiring information about any U.S. person's domestic activities.

(b) The foreign intelligence cannot be reasonably obtained from publicly available information or from sources who are advised, or are otherwise aware, that they are providing information to DoD or a Defense Intelligence Component.

(c) DIRNSA/CHCSS or a single delegee has approved, as being consistent with this issuance, the use of techniques other than the collection of information from publicly available information or from sources who are advised or are otherwise aware that they are providing information to DoD or a Defense Intelligence Component. NSA/CSS will provide a copy of any such approval to the USD(I&S) and the DoD SIOO.

3.3. PROCEDURE 3. RETENTION OF USPI.

a. Scope. This procedure governs the retention of USPI collected by NSA/CSS in accordance with Procedure 2. Paragraphs 3.3.d through 3.3.h govern information that does not fall within the definition of collection because it was disseminated by another Component or element of the Intelligence Community. This procedure does not apply to the retention of information obtained under FISA, which has its own provisions.

b. Definition of Terms. See the Glossary for the definition of "administrative purposes," "CI," "Defense Intelligence Component employee," "dissemination," "foreign intelligence," "incidental collection of USPI," "intentional collection of USPI," "retention," "U.S. person," and "USPI."

c. Evaluation of Information. NSA/CSS will evaluate information that may contain USPI to determine whether it may be permanently retained under Paragraph 3.3.e. as follows:

(1) Intentional Collection of USPI. If NSA/CSS intentionally collects USPI, NSA/CSS will evaluate the information promptly. If necessary, NSA/CSS may retain the information for evaluation for up to 5 years. DIRNSA/CHCSS or a single delegee may approve an extended period in accordance with Paragraph 3.3.c.(5).

(a) Collection about a person reasonably believed to be in the United States. NSA/CSS may intentionally collect information about a person or object that, at the time of collection, is in the United States or about a place in the United States. If NSA/CSS does so and incidentally may have collected USPI about a person other than the subject of intentional collection, NSA/CSS may retain all of the collected information for evaluation for up to 5 years. DIRNSA/CHCSS or a single delegee may approve an extended period in accordance with Paragraph 3.3.c.(5).

(b) Collection about a person reasonably believed to be outside the United States. NSA/CSS may intentionally collect information about a person or object that, at the time of collection, is outside the United States or about a place outside the United States. If NSA/CSS does so and incidentally may have collected USPI about a person other than the subject of intentional collection, NSA/CSS may, subject to Paragraph 3.3.c.(5)(b), retain all of the incidentally collected information for evaluation for up to 25 years.

(3) Voluntarily Provided USPI. If NSA/CSS receives information that is voluntarily provided about a person reasonably believed to be a U.S. person, NSA/CSS will evaluate the information promptly. If necessary, NSA/CSS may retain the information for evaluation for up to 5 years. DIRNSA/CHCSS or a single delegee may approve an extended period in accordance with Paragraph 3.3.c.(5). If NSA/CSS receives information that is voluntarily provided about a person reasonably believed to be a non-U.S. person, but the information may contain USPI, NSA/CSS may, subject to Paragraph 3.3.c.(5)(b), retain the information for evaluation for up to 25 years.

(4) Special Circumstances. If NSA/CSS conducts a special circumstances collection in accordance with Procedure 2.e, NSA/CSS may retain the information for evaluation for up to 5 years. If a special circumstances collection involves the intentional collection of USPI, that information will be promptly evaluated and, if necessary, may be retained for up to 5 years. The USD(I&S) may approve an extended period in accordance with Paragraph 3.3.c.(5).

(5) Extended Retention.

(a) General Requirements. DIRNSA/CHCSS or a single delegee or the USD(I&S), as appropriate, may approve, either at the time of collection or thereafter, the further retention of specific information or categories of information subject to Paragraphs 3.3.c.(1), 3.3.c.(2)(a), 3.3.c.(3), or 3.3.c.(4) for no more than 5 years beyond the time permitted in those paragraphs.

1. The official must find that the retention is necessary to carry out an authorized mission of NSA/CSS; find that NSA/CSS will retain and handle the information in a manner consistent with the protection of privacy and civil liberties; consider the need for enhanced protections, such as those described in Paragraph 3.3.g.(2); and consult with legal and privacy and civil liberties officials.

2. In determining whether to approve an extended retention period, the official must also find that the information is likely to contain valuable information that NSA/CSS is authorized to collect in accordance with Procedure 2.

3. The official must document compliance with the requirements of this paragraph in writing. Any further extension of retention beyond the limits specified in Paragraph 3.3.c. must be addressed as an exception to policy in accordance with Paragraph 3.1.d.

(b) Additional Requirements for Certain Communications. In addition to complying with Paragraph 3.3.c.(5)(a), if NSA/CSS wants to retain telephone or electronic communications subject to Section 1813 of Title 50, U.S.C. (also known as Section 309 of the 2015 Intelligence Authorization Act) for more than 5 years, NSA/CSS must also comply with the requirements of Section 1813(b)(3)(B) of Title 50, U.S.C.

(6) Unintelligible Information. For any information that is not in an intelligible form, the time periods identified in Paragraph 3.3.c. begin when the information is processed into intelligible form. Unintelligible information includes information that NSA/CSS cannot decrypt or understand in the original format. To the extent practicable, unintelligible information will be processed into an intelligible form.

(7) Deletion of Information. Unless NSA/CSS determines that USPI covered by Paragraph 3.3.c. meets the standards for permanent retention during the specified time period, NSA/CSS must delete all USPI (including any information that may contain USPI) from NSA/CSS's automated systems of records.

d. Information Disseminated by Another Component or Intelligence Community Element. If another Component or element of the Intelligence Community disseminates unevaluated information that may contain USPI to NSA/CSS, the recipient Component may only retain the information and evaluate it for permanent retention pursuant to Paragraph 3.3.e. for as long as the originating agency may retain it. If the disseminating Component or element has already determined that the information meets Attorney General-approved standards for permanent retention, then NSA/CSS must only verify that the information is reasonably believed to be necessary for the performance of NSA/CSS's authorized intelligence mission in order to permanently retain the information.

e. Permanent Retention.

(1) Retention Standard. Subject to Paragraphs 3.3.f. and 3.3.g., NSA/CSS may permanently retain USPI if it determines that retention is reasonably believed to be necessary for the performance of an authorized intelligence mission or function and the USPI falls into one or more of the following categories:

(a) The information was lawfully collected by NSA/CSS or disseminated to NSA/CSS by another Component or element of the Intelligence Community and meets a collection category in Paragraph 3.2.c.

(b) The information was collected by NSA/CSS incidentally to authorized collection or disseminated to NSA/CSS by another Component or element of the Intelligence Community, and is necessary to understand or assess foreign intelligence or CI, such as information about a U.S. person that provides important background or context for foreign intelligence or CI.

(2) Retention for Oversight. NSA/CSS may permanently retain USPI for purposes of oversight, accountability, or redress; when required by law or court order; or when directed by the DoD SIOO, NSA/CSS Inspector General, or the Attorney General.

(3) Retention of Specific USPI. NSA/CSS will determine whether information that contains USPI meets the standard for permanent retention at the most specific level of information that is appropriate and practicable.**f. Protections for USPI.**

(1) Responsibilities of NSA/CSS. NSA/CSS will implement the following measures to protect USPI:

(a) Limit access to and use of such information to those employees who have appropriate security clearances, accesses, and a mission requirement.

(b) When retrieving information electronically:

1. Only use queries or other techniques that are relevant to the intelligence mission or other authorized purposes.

2. Tailor queries or other techniques to the greatest extent practicable to minimize the amount of USPI returned that is not pertinent to the intelligence mission and purpose for the query.

3. Establish written procedures to document the basis for conducting a query of unevaluated information that is intended to reveal USPI.

(c) Take reasonable steps to audit access to information systems containing USPI and to periodically audit queries or other search terms to assess compliance with this issuance.

(d) In developing and deploying information systems that are used for intelligence involving USPI, take reasonable steps to ensure effective auditing and reporting as required by this issuance.

(e) Establish documented procedures for retaining data containing USPI and recording the reason for retaining the data and the authority approving the retention.

(f) In accordance with DoD or NSA/CSS policy, annually train employees who access or use USPI on the civil liberties and privacy protections that apply to such information.

(2) Marking Electronic and Paper Files. NSA/CSS will use reasonable measures to identify and mark or tag 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, NSA/CSS will also mark files and documents containing USPI individually. In the case of certain electronic databases, if it is not reasonably possible to mark individual files containing USPI, NSA/CSS may use a banner informing users before access that they may encounter USPI.

(3) Reviews. The DoD SIOO or other designated oversight personnel will periodically:

(a) Review NSA/CSS practices for protecting USPI in accordance with this procedure.

(b) Evaluate the adequacy of temporary retention periods established in Paragraph 3.3.c.

g. Enhanced Safeguards.

(1) Determining Need for Enhanced Safeguards. Whenever there is a special circumstance collection in accordance with Paragraph 3.2.e, DIRNSA/CHCSS or delegee will consider all of the following factors to assess whether there is a need for enhanced retention safeguards to protect USPI:

(a) The intrusiveness of the methods used by NSA/CSS or others to acquire the USPI.

(b) The volume, proportion, and sensitivity of the USPI being retained.

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

(d) The uses of the information being retained and the types of queries or searches expected to be conducted.

(e) The length of time the information will be retained.

(f) Practical and technical difficulties associated with implementing any enhanced safeguards.

(g) Any legal or policy restrictions that apply to the information, including Section 552a of Title 5, U.S.C. also known as “the Privacy Act of 1974.”

(h) Other factors as directed by the USD(I&S).

(2) Implementation of Enhanced Safeguards. If DIRNSA/CHCSS or delegee determines that there is a need for enhanced safeguards, he or she will consider and identify for implementation any of the following measures deemed appropriate:

(a) Procedures for review, approval, or auditing of any access or searches.

(b) Procedures to restrict access or dissemination, including limiting the number of personnel with access or authority to search; establishing a requirement for higher-level approval or legal review before or after access or search; or requiring higher-level approval or legal review before or after USPI is unmasked or disseminated.

(c) Use of privacy-enhancing techniques, such as information masking that indicates the existence of USPI without providing the content of the information, until the appropriate approvals are granted.

(d) Access controls, including data segregation, attribute-based access, or other physical or logical access controls.

(e) Additional training requirements.

(f) Additional protective retention measures.

h. Maintenance and Disposition of Information. The maintenance and disposition of USPI that is retained in the files of NSA/CSS will conform to this procedure and to NSA/CSS records management schedules approved by the Archivist of the United States for the files or records in which the information is retained.

i. Signals Intelligence (SIGINT). Any retention of USPI obtained from SIGINT is subject to the procedures in the classified annex to this issuance and any applicable Presidential directives.

3.4. PROCEDURE 4. DISSEMINATION OF USPI

a. Scope. This procedure governs the dissemination of USPI collected or retained by NSA/CSS. Information may be disseminated pursuant to this procedure only if it was properly collected or retained in accordance with Procedures 2 or 3. This procedure applies to USPI in any form, including physical and electronic files and information NSA/CSS places in databases, on websites, or in shared repositories accessible to other persons or organizations outside NSA/CSS. This procedure does not apply to the dissemination of information collected solely for administrative purposes, or disseminated pursuant to other procedures approved by the Attorney General or a court order that otherwise imposes controls on such dissemination.

b. Definition of Terms. See the Glossary for the definitions of "administrative purposes," "CI," "consent," "Defense Intelligence Component employee," "dissemination," "publicly available," "shared repository," "U.S. person," and "USPI."

c. Criteria for Dissemination. Subject to the other paragraphs of this procedure, USPI may only be disseminated by NSA/CSS employees who have received training on this procedure and if the information falls into one or more of the following categories:

(1) Any Person or Entity. The dissemination is to any person or entity and the information is publicly available or the information concerns a U.S. person who has consented to the dissemination.

(2) Other Intelligence Community Elements. The dissemination is to another appropriate element of the Intelligence Community (including another Defense Intelligence Component) for the purpose of allowing the recipient to determine whether the information is relevant to its responsibilities and can be retained by it in accordance with its procedures approved by the Attorney General or, in the case of DoD Components, this issuance.(3) Other DoD Elements. The dissemination is to an element of DoD (including a DoD contractor) and the recipient is reasonably believed to have a need to receive such information for the performance of its lawful missions or functions.

(4) Other Federal Government Entities. The dissemination is to any other part of the Federal Government and the recipient is reasonably believed to have a need to receive such information for the performance of its lawful missions or functions. (5) State, Local, Tribal, or Territorial Governments. The dissemination is to a State, local, tribal, or territorial government and the recipient is reasonably believed to have a need to receive such information for the performance of its lawful missions or functions.(6) Foreign Governments or International Organizations. The dissemination meets all of the following requirements:(a) The dissemination is to a foreign government or an international organization;

(b) The recipient is reasonably believed to have a need to receive such information for the performance of its lawful missions or functions; and

(c) DIRNSA/CHCSS or a delegee has determined that the disclosure is consistent with applicable international agreements and foreign disclosure policy and directives, including those policies and directives requiring protection against the misuse or unauthorized dissemination of information, and the analysis of potential harm to any individual.

(7) Assistance to NSA/CSS. The dissemination is to a governmental entity, an international entity, or an individual or entity not part of a government and is necessary for the limited purpose of assisting NSA/CSS in carrying out an authorized mission or function. Any dissemination to a foreign government or international organization must also comply with Paragraph 3.4.c.(6). For a dissemination under this paragraph, NSA/CSS will inform the recipient that it should do all of the following, except in exceptional circumstances where providing such information is inconsistent with operational requirements, as determined by DIRNSA/CHCSS or a delegee:(a) Only use the information for this limited purpose;

(b) Properly safeguard the information;

(c) Return or destroy the information when it has provided the requested assistance; and

(d) Not disseminate the information further without the prior approval of NSA/CSS.

(8) Protective Purposes. The dissemination is to a governmental entity, an international organization, or an individual or entity not part of a government, and is necessary to protect the safety or security of persons or property, or to protect against or prevent a crime or threat to the national security. For any dissemination of USPI to individuals or entities not part of a government, DIRNSA/CHCSS or a delegee will assess the risk associated with such dissemination, consider whether any further restrictions or handling caveats are needed to protect the information, and comply with any limitations required by foreign disclosure policy. A dissemination to a foreign government or international organization must also comply with Paragraph 3.4.c.(6).

(9) Required Disseminations. The dissemination is required by statute; treaty; Executive order; Presidential directive; National Security Council guidance; policy, memorandum of understanding, or agreement approved by the Attorney General; or court order. **d. Disseminations of Large Amounts of Unevaluated USPI.** If NSA/CSS wants to disseminate a large amount of USPI in accordance with Paragraphs 3.4.c.(3) through 3.4.c.(8) that has not been evaluated to determine whether it meets the standard for permanent retention, DIRNSA/CHCSS or a single delegee must approve the dissemination, after notifying the DoD SIOO .

(1) The approving official must find that the dissemination complies with the other requirements of this procedure and that it is not reasonably possible to accomplish the intended objective by disseminating a lesser amount of USPI.

(2) If the recipient is outside the Federal Government, the recipient must represent that it has appropriate protections in place, comparable to those required by Paragraphs 3.3.f and 3.3.g, to safeguard and monitor USPI and to comply with applicable laws; that it will use the information for lawful purposes; and that it will access and retain the information only for those purposes.

e. Minimization of Dissemination Content. To the extent practicable, NSA/CSS should not include USPI in a dissemination (other than a dissemination pursuant to Paragraph 3.4.c.(1) or (2)) if the pertinent information can be conveyed in an understandable way without including the identifying information. If a dissemination includes USPI, NSA/CSS will notify the recipient so the recipient can protect the USPI appropriately.

f. Disseminations Requiring Approval. For any dissemination under Paragraph 3.4.c.(4) through (6) that is not for foreign intelligence, CI, security, law enforcement, cybersecurity, humanitarian assistance, disaster relief, threats to safety, or protective purposes, DIRNSA/CHCSS or delegee must approve the dissemination.

g. Dissemination of SIGINT. The dissemination of information derived from SIGINT must also comply with the requirements of Procedure 5.

h. Improper Dissemination of USPI. NSA/CSS will develop procedures to address instances of improper dissemination of USPI, including required reporting.

i. Dissemination Not Conforming to This Procedure. Any proposed dissemination that does not conform to the requirements of this procedure must be approved by DIRNSA/CHCSS on the advice of the NSA OGC, after consultation with the GC DoD and the National Security Division of the Department of Justice, and the NSA/CSS CLPT. Such approval will be based on a determination that the proposed dissemination complies with applicable laws, Executive orders, and regulations.

3.5. PROCEDURE 5. ELECTRONIC SURVEILLANCE.

a. Scope. This procedure implements the Foreign Intelligence Surveillance Act (FISA) and E.O. 12333. NSA/CSS may conduct electronic surveillance for an intelligence purpose in accordance with FISA or E.O. 12333 and this procedure. The legal framework for conducting electronic surveillance is dependent upon NSA/CSS's mission, the U.S. person status and location of the target, the methods used to conduct the electronic surveillance, and the type of communication sought. All electronic surveillance must also comply with Procedures 1 through 4 of this issuance.

(1) Need for Guidance. The authorities governing electronic surveillance are complex and subject to change. This procedure addresses the situations that most frequently arise and, even for those situations, only describes some of the legal requirements. Accordingly, NSA/CSS personnel should seek the guidance of legal counsel when planning and conducting electronic surveillance.

(2) Other Legal Authorities. In addition to the legal authorities discussed in this procedure, other authorities, Sections 1841-1846 of Title 50, U.S.C., and Sections 3121-3127 of Title 18, U.S.C., exist for the use of pen register and trap-and-trace devices, which are devices used to obtain dialing, routing, addressing, or signaling information such as telephone numbers or e-mail addresses. Sections 2510-2522 of Title 18, U.S.C. also govern electronic surveillance conducted as part of a criminal investigation.

(3) Definition of Terms. For definitions of "CI," "consent," "dissemination," "electronic surveillance," "foreign intelligence," "foreign power," "radio communications hearability survey," "reasonable expectation of privacy," "retention," "technical surveillance countermeasures (TSCM)," "transmission media vulnerability survey," "United States," "U.S. person," and "USPI," see the Glossary. In addition, for purposes of this procedure, the term "Attorney General" includes the Acting Attorney General, the Deputy Attorney General, or the Assistant Attorney General for National Security.

b. Compliance with the Fourth Amendment. All electronic surveillance must comply with the Fourth Amendment to the Constitution. NSA OGC (D2) will assess the reasonableness of collection and restrictions on the retention and dissemination of USPI to ensure protection of Fourth Amendment rights and, when necessary, will consult with NSA/CSS CLPT (D5) officials and the Department of Justice.

c. Electronic Surveillance Targeting a Person in the United States. NSA/CSS may conduct electronic surveillance targeting a person in the United States only for foreign intelligence or CI purposes. FISA governs such activities, except in very limited circumstances and in accordance with this procedure.

(1) Legal References. For FISA's applicability to electronic surveillance targeting a person in the United States, see Sections 101-112 of FISA (Sections 1801-1812 of Title 50, U.S.C.).

(2) Procedures. Only the Attorney General or a judge of the Foreign Intelligence Surveillance Court (FISC) may authorize electronic surveillance, as that term is defined in FISA, for intelligence purposes in the United States, except for emergency situations in accordance with Paragraph 3.5.g. NSA/CSS must comply with the requirements of FISA and, in most circumstances, may only conduct such surveillance if both:

(a) A significant purpose of the electronic surveillance is to obtain foreign intelligence information, as the terms "electronic surveillance" and "foreign intelligence information" are defined in FISA; and

(b) There is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power, as the terms "electronic surveillance," "foreign power," and "agent of a foreign power" are defined in FISA.

(3) Authority to Request Electronic Surveillance Under This Section. Authority to approve the submission of applications or requests for electronic surveillance as that term is defined in FISA is limited to the Secretary of Defense, the Deputy Secretary of Defense, the USD(I&S), the Secretary or Under Secretary of a Military Department, or the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS). Applications to the FISC will be made through the Attorney General after being cleared by the GC DoD.

d. Electronic Surveillance Targeting a U.S. Person Outside the United States. FISA and E.O. 12333 govern electronic surveillance conducted by NSA/CSS targeting a U.S. person who is outside the United States.

(1) Legal References. For electronic surveillance under FISA targeting a U.S. person outside the United States, see Sections 101-112, 703, 704, and 705 of FISA (Sections 1801-1812 and 1881b-d of Title 50, U.S.C.). Section 2.5 of E.O. 12333 also applies to electronic surveillance targeting a U.S. person outside the United States.

(2) Procedures. When conducting electronic surveillance targeting a U.S. person outside the United States, NSA/CSS must comply with both of the following:

(a) The electronic surveillance must have been authorized under FISA or Section 2.5 of E.O. 12333, or both, as appropriate; and

(b) There must be probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power, as the terms "electronic surveillance," "foreign power," and "agent of a foreign power" are defined in FISA or, in some circumstances, an officer or employee of a foreign power.

(3) Authority to Request Electronic Surveillance Under This Section. Authority to approve the submission of applications or requests for electronic surveillance under FISA or Section 2.5 of E.O. 12333 is limited to the Secretary of Defense, the Deputy Secretary of Defense, the USD(I&S), the Secretary or Under Secretary of a Military Department, or the DIRNSA/CHCSS. Applications to the FISC for orders are made through the Attorney General after being cleared by the GC DoD, except that applications for court orders pursuant to Sections 703, 704, or 705(a) of FISA may be submitted through the Attorney General after being cleared by the National Security Agency Office of General Counsel (NSA OGC).

e. Electronic Surveillance Under FISA Targeting a Non-U.S. Person Outside the United States.

(1) Procedures. NSA/CSS may request authorization for electronic surveillance targeting a non-U.S. person who is outside the United States under the following FISA authorities:

(a) Title I. This title of FISA applies if NSA/CSS is seeking to conduct electronic surveillance as that term is defined in FISA. See Sections 101-112 of FISA (Sections 1801-1812 of Title 50, U.S.C.). The FISC or the Attorney General may approve an application or request for electronic surveillance of a foreign power or an agent of a foreign power, as those terms are defined in FISA, based on a finding that the application or request satisfies the requirements of Sections 1802(a) or 1804(a) of Title 50, U.S.C.

(b) Section 702. This section of FISA may be used to obtain foreign intelligence information from or with the assistance of an electronic communication service provider. NSA/CSS may conduct surveillance in accordance with Section 702 only in accordance with a joint certification from the Attorney General and the Director of National Intelligence, with review by the FISC. For information on electronic surveillance in accordance with Section 702, contact the NSA OGC or the GC DoD. For additional information, see Section 1881a of Title 50, U.S.C.

(2) Authority to Request Electronic Surveillance Under This Section. Authority to approve the submission of applications or requests for electronic surveillance in accordance with Title I of FISA is limited to the Secretary of Defense, the Deputy Secretary of Defense, the USD(I&S), the Secretary or Under Secretary of a Military Department, or the DIRNSA/CHCSS. Applications to the FISC for court orders are made through the Attorney General after being cleared by the GC DoD.

f. Electronic Surveillance Under Executive Branch Authority. NSA/CSS may conduct electronic surveillance in accordance with this section only for an authorized foreign intelligence, CI, or support to military operations purpose. Such surveillance must be conducted

in accordance with E.O. 12333, other Presidential directives, this issuance, and the classified annex to this issuance. Such surveillance involves the collection of foreign communications. It may result in the incidental collection of USPI or the collection of communications to or from the United States. To ensure that such surveillance is properly conducted, the DIRNSA/CHCSS or a delegee will issue appropriate directives and instructions implementing this issuance and the classified annex to govern the conduct of the U.S. SIGINT System (USSS).

g. Electronic Surveillance in Emergency Situations.

(1) In accordance with FISA or Section 2.5 of E.O. 12333, NSA/CSS may conduct electronic surveillance in emergency situations with the approval of the Attorney General. Authority to request emergency electronic surveillance is limited to the Secretary of Defense, the Deputy Secretary of Defense, the USD(I&S), the Secretary or Under Secretary of a Military Department, or the DIRNSA/CHCSS. DIRNSA/CHCSS or a delegee may request that the GC DoD seek authorization directly from the Attorney General if it is not feasible to submit such a request through one of these officials. Under this circumstance, DIRNSA/CHCSS or a delegee will notify the appropriate official as soon as possible. For surveillance proposed by the DIRNSA/CHCSS, the NSA OGC will request the Attorney General's approval.

(2) In addition, if NSA/CSS is conducting electronic surveillance of a non-U.S. person outside the United States in accordance with Section 702 of FISA and that person enters the United States, under very limited circumstances DIRNSA/CHCSS may authorize continued surveillance of that person for up to 72 hours in accordance with Section 1805(f) of Title 50, U.S.C. Refer questions about this provision to the NSA OGC or to the GC DoD.

h. Exigent Circumstances Involving a U.S. Person Outside the United States.

(1) Legal Standard. NSA/CSS may conduct electronic surveillance targeting a U.S. person outside the United States in exigent circumstances when securing the prior approval of the Attorney General is not practical and one or more of the following conditions exists:

(a) A person's life or physical safety is reasonably believed to be in imminent danger;

(b) The physical security of a defense installation or government property is reasonably believed to be in imminent danger; in this situation, the approving official must determine that there is probable cause to believe that the targeted U.S. person is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power; or

(c) The time required would cause failure or delay in obtaining significant foreign intelligence or CI, and such failure or delay would result in substantial harm to the national security. In this situation, the approving official must determine that there is probable cause to believe that the targeted U.S. person is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power.

(2) Authority to Approve. Authority to approve electronic surveillance involving exigent circumstances is limited to the Secretary of Defense; the Deputy Secretary of Defense; the USD(I&S); the Secretary or Under Secretary of a Military Department; the DIRNSA/CHCSS; the NSA Deputy Director; a single delegee designated by the DIRNSA/CHCSS; the DIRNSA/CHCSS' senior representative present; or any general or flag officer at the overseas location in question who has responsibility for the subject of the surveillance or for the protection of the persons, installations, or property that is endangered. Such official will promptly notify the GC DoD or the NSA OGC, as appropriate, of any such surveillance, the reason for authorizing the surveillance on an exigent basis, and the expected results. The GC DoD or the NSA OGC will notify the Attorney General as soon as possible of the surveillance, the circumstances surrounding its authorization, and the results thereof, and provide information as may be needed to authorize continuation of the surveillance.

(3) Time Limit. Authorized electronic surveillance may continue for the amount of time required for a decision by the Attorney General, but may not continue for longer than 72 hours without the Attorney General's approval.

i. Electronic Surveillance Activities Subject to Special Provisions. Personnel of **NSA/CSS** may also conduct electronic surveillance when:

(1) Developing, Testing, and Calibrating Electronic Equipment.

(a) Applicability. This section applies to developing, testing, and calibrating electronic equipment that can intercept or process communications and non-communications signals. It also includes research and development that needs electronic communications as a signal source and implements Section 105(g)(1) of FISA (Section 1805(g)(1) of Title 50, U.S.C.).

(b) Signals That May Be Used Without Restriction:

1. Laboratory-generated signals, whether acquired inside or outside a laboratory.

2. Communications signals acquired with the consent of one of the communicants.

3. Communications in the commercial or public service broadcast bands.

4. Communications transmitted between terminals located outside the United States not used by any known U.S. person and that are either collected outside the United States or collected inside the United States in a manner that does not constitute electronic surveillance as that term is defined in FISA.

5. Non-communications signals.

(c) Signals That May Be Used With Minimization Procedures. Communications subject to lawful electronic surveillance in accordance with FISA or E.O. 12333 for foreign

intelligence or CI purposes may be used subject to the minimization procedures applicable to such surveillance.

(d) Signals That May Only Be Used With the Restrictions Set Out in Paragraph 3.5.i.(1)(e):

1. Communications over official government communications circuits with consent from an appropriate official of the controlling agency.

2. Communications in the citizens and amateur-radio bands.

3. Other signals may be used only when it is determined that it is not practical to use the signals described in Paragraphs 3.5.i.(1)(d)1 and 2 and it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance. The Attorney General must approve use of signals pursuant to this paragraph when the period of use exceeds 90 days. When the Attorney General's approval is required, NSA/CSS will submit a test proposal to the NSA OGC or the GC DoD. The test proposal will state the requirement for a test beyond 90 days, the nature of the activity, the organization that will conduct the activity, and the proposed disposition of any signals or communications acquired during the activity.

(e) Restrictions.

1. Scope. The activities authorized in Paragraph 3.5.i.(1)(d) will be limited in scope and duration to that necessary to develop, test, and calibrate electronic equipment.

2. Targeting. The activities will not intentionally target any particular person or persons.

3. Retention, Use, and Dissemination.

a. Government Signals and Signals in the Citizens and Amateur-Radio Bands. The technical parameters of a communication (e.g., frequency, modulation, bearing, signal strength, and time of activity) may be retained and used only for developing, testing, and calibrating electronic equipment or for collection avoidance purposes. Technical parameters may be disseminated to other Defense Intelligence Components and to other entities authorized to conduct electronic surveillance or related development, testing, and calibration of electronic equipment, provided that such dissemination and use are only for developing, testing, and calibrating electronic equipment or for collection avoidance purposes. For purposes of this paragraph, the content of a communication is information about the substance, purport, or meaning of the communication. The content of a communication acquired in accordance with Paragraph 3.5.i.(1)(d)1 or 2 may be retained or used only when needed for developing, testing, and calibrating electronic equipment; may only be disclosed to persons conducting the activity; and must be destroyed before or immediately upon completion of the activity.

b. Signals Collected under Paragraph 3.5.i.(1)(d)3. The technical parameters of a communication (e.g., frequency, modulation, bearing, signal strength, and time of activity)

may be retained and used only for developing, testing, and calibrating electronic equipment or for collection avoidance purposes. Technical parameters may be disseminated to other Defense Intelligence Components and to other entities authorized to conduct electronic surveillance or related development, testing, and calibration of electronic equipment, provided that such dissemination and use are only for developing, testing, and calibrating electronic equipment or for collection avoidance purposes. The content of a communication acquired pursuant to Paragraph 3.5.i.(1)(d)3 may be retained or used only when needed for developing, testing, and calibrating electronic equipment; may only be disclosed to persons conducting the activity; and must be destroyed before or immediately upon completion of the activity. For purposes of this paragraph, the content of a communication is information about the substance, purport, meaning, or existence of the communication (as defined in Section 1801(n) of Title 50, U.S.C.). These activities will also be conducted in accordance with Sections 2510-2522 of Title 18, U.S.C. (also known as the Wiretap Act), Sections 3121-3127 of Title 18, U.S.C. (also known as the Pen Register and Trap and Trace Devices Act), and FISA.

(2) Technical Surveillance Countermeasures (TSCM)

(a) Applicability. This section applies to the use of electronic equipment and specialized techniques to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance. It implements Section 105(g)(2) of FISA (Section 1805(g)(2) of Title 50, U.S.C.).

(b) Procedures. TSCM may only be conducted by organizations approved by the USD(I&S). The use of TSCM equipment by NSA/CSS may involve the incidental acquisition of information without consent of those subjected to the surveillance, provided the use comports with all of the following conditions:

1. It is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

2. The use of TSCM is limited in extent and duration to that necessary to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance;

3. The use of TSCM has been authorized or consented to by the official in charge of the facility, organization, or installation where the countermeasures are to be undertaken; and

4. If the use of TSCM constitutes electronic surveillance as that term is defined in FISA, such countermeasures are not targeted against the communications of any particular person or persons.

(c) Retention and Dissemination of Information Acquired During TSCM Activities.

1. In conducting TSCM, NSA/CSS may only retain or disseminate information that is acquired in a manner that constitutes electronic surveillance as that term is defined in

FISA to protect information from unauthorized surveillance or to enforce Chapter 119 of Title 18 and Section 605 of Title 47, U.S.C. Any information acquired must be destroyed when no longer required for these purposes or as soon as is practicable.

2. If the information is acquired in a manner that does not constitute electronic surveillance as that term is defined in FISA, the information may be retained and disseminated in accordance with Procedures 3 and 4.

3. The technical parameters of a communication (e.g., frequency, modulation, bearing, signal strength, and time of activity) may be retained and used for the purposes described in the Paragraph 3.5.i.(2)(a) or for collection avoidance purposes. The technical parameters will be maintained in accordance with NSA/CSS Records Management Schedules.

4. A record of the types of communications and information subject to acquisition by unauthorized electronic surveillance that is detected by the TSCM activity may be retained.

(3) Training of Personnel in the Operation and Use of Electronic Surveillance Equipment.

(a) Applicability. This section applies to NSA/CSS training of personnel in the operation and use of electronic surveillance equipment. It implements Section 105(g)(3) of FISA (Section 1805(g)(3) of Title 50, U.S.C.).

(b) Training Guidance. The training of personnel by NSA/CSS in the operation and use of electronic surveillance equipment will include guidance concerning the requirements and restrictions of FISA and E.O. 12333 with respect to the unauthorized acquisition and use of communications and information.

(c) Preferred Signals for Training Purposes. To the maximum extent practical, use of electronic surveillance equipment for training purposes will be directed against:

1. Communications that are subject to lawful electronic surveillance for foreign intelligence and CI purposes.

2. Public broadcasts, distress signals, or official U.S. Government communications provided that, when government agency communications are monitored, the consent of an appropriate official is obtained.

3. Laboratory-generated signals, whether acquired inside or outside a laboratory.

4. Communications signals acquired with the consent of one of the communicants.

5. Communications transmitted between terminals located outside the United States not used by any known U.S. person and that are either collected outside the United States or collected inside the United States in a manner that does not constitute electronic surveillance as that term is defined in FISA.

6. Non-communications signals.

(d) Use of Other Signals for Training Purposes. If it is not practical to train personnel in the use of electronic surveillance equipment using the communications described in Paragraphs 3.5.i.(3)(c)1 through 6 as preferred signals for training purposes, NSA/CSS may engage in electronic surveillance as that term is defined in FISA to train personnel if all of the following conditions are met:

1. The surveillance is not targeted at the communications of any particular person or persons without consent;

2. It is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

3. It is not reasonable to train personnel in the use of such equipment without engaging in electronic surveillance as that term is defined in FISA;

4. The electronic surveillance is limited in extent and duration to that necessary to train personnel in the use of the equipment; and

5. Minimal acquisition of information is permitted as required for calibration purposes.

(e) Retention and Dissemination. Information collected during training that involves communications subject to lawful electronic surveillance for foreign intelligence and CI purposes will be retained and disseminated to the extent permitted by the applicable minimization procedures and maintained in accordance with NSA/CSS Records Management Schedules. Information collected during training that does not involve such communications will be destroyed as soon as practical or upon completion of the training and may not be disseminated for any purpose. This limitation does not apply to distress signals.

j. Transmission Media Vulnerability and Radio Communications Hearability Surveys. This section applies to the conduct of transmission media vulnerability surveys and radio communications hearability surveys; it does not apply to TSCM.

(1) Transmission Media Vulnerability Surveys. With prior written authorization of the DIRNSA/CHCSS or a delegee, National Security Agency/Central Security Service (NSA/CSS) may conduct surveys of transmission facilities of communications common carriers, other private commercial entities, and U.S. Government entities to determine the potential vulnerability to interception by foreign intelligence services, subject to the following limitations:

(a) Collection: When practicable, before a transmission media vulnerability survey begins, NSA/CSS must obtain authorization or consent from the official in charge of the facility, organization, or installation where the survey is to be conducted.

(b) Processing and Retention: Information collected during a transmission media vulnerability survey must be processed and retained as follows:

1. No transmission may be acquired aurally, except for transmissions to or from U.S. Government entities acquired in accordance with other procedures approved by the Attorney General.

2. No content of any transmission may be acquired by any means. For purposes of this paragraph, the content of a communication is information about the substance, purport, meaning, or existence of the communication. This limitation does not apply to the content of transmissions that are directed at or that may connect to a U.S. Government entity's facilities, when such transmissions are acquired by that entity. These activities will also be conducted in accordance with the Sections 2510-2522 of Title 18, U.S.C. (also known as the Wiretap Act), Sections 3121-3127 of Title 18, U.S.C. (also known as the Pen Register and Trap and Trace Devices Act), and FISA.

3. No transmissions may be recorded, except those acquired in accordance with Paragraph 3.5.j.(1)(b)1 or 2.

4. No report or log may include USPI, except for the purpose of identifying transmission facilities that are vulnerable to surveillance by foreign powers. If the users of such facilities are not also the facilities' owners, the identities of the users may be obtained and may be included in a report or log. However, the identities of such users may not be obtained from the content of the transmissions themselves, including information about the existence of a specific communication, except for identities acquired in accordance with Paragraph 3.5.j.(1)(b)1 or 2.

(c) Dissemination: Reports may be disseminated in accordance with Procedure 4. Logs may be disseminated in accordance with Procedure 4 only if required to verify results contained in reports.

(2) Radio Communications Hearability Surveys. With the prior written approval of the DIRNSA/CHCSS or a delegee, NSA/CSS may conduct radio communications hearability surveys of telecommunications that are transmitted in the United States, subject to the following limitations:

(a) Collection. When practicable, before a radio communications hearability survey begins, NSA/CSS must obtain authorization or consent from the official in charge of the facility, organization, or installation where the survey is to be conducted.

(b) Processing and Retention. Information collected during a radio communications hearability survey must be processed and retained as follows:

1. The content of communications may not be recorded or included in any report or log. For purposes of this paragraph, the content of a communication is information about the substance, purport, meaning, or existence of the communication. These activities will also be

conducted in accordance with Sections 2510-2522 of Title 18, U.S.C. (also known as the Wiretap Act), Sections 3121-3127 of Title 18, U.S.C. (also known as the Pen Register and Trap and Trace Devices Act), and FISA.

2. No microwave transmission may be de-multiplexed or demodulated for any purpose.

3. No report or log may identify any person or entity, except for the purpose of identifying the transmission facility that can be intercepted from the intercept site. If the users of such facilities are not also the facilities' owners, and the identities of the users are relevant to the purpose of the survey, the identities of the users may be obtained. However, the identities of the users may not be obtained from the content of the transmissions themselves, including information about the existence of a specific communication.

(c) Dissemination. Reports may be disseminated in accordance with Procedure 4 and only within the U.S. Government. Logs may be disseminated in accordance with Procedure 4 only if required to verify results contained in reports.

k. Military Tactical Exercise Communications. These are U.S. and allied military exercise communications within the United States and abroad necessary either for the production of simulated foreign intelligence and CI or to permit an analysis of communications security. The U.S. SIGINT System may collect, process, retain, and disseminate military tactical exercise communications that contain USPI only in accordance with the classified annex to this issuance.

(1) Collection. Collection efforts will be conducted in the same manner as in the case of SIGINT for foreign intelligence purposes and must be designed to avoid to the extent feasible the interception of communications not related to military exercises.

(2) Processing and Retention.

(a) Military tactical exercise communications may be retained and processed without deletion of references to U.S. persons who are participants in, or are otherwise mentioned in, exercise-related communications.

(b) Inadvertently intercepted communications of U.S. persons not participating in the exercise will be destroyed as soon as feasible in accordance with NSA/CSS's disposition schedule.

(3) Dissemination. Dissemination of military tactical communications and exercise reports or information files derived from such communications will be limited to those authorities and persons participating in or conducting reviews and critiques of such exercises.

3.6. PROCEDURE 6. CONCEALED MONITORING. *DOES NOT PERTAIN TO NSA/CSS*

a. Scope.

(1) This procedure governs concealed monitoring of any person inside the United States or any U.S. person outside the United States for an authorized foreign intelligence or CI purpose by a Defense Intelligence Component or anyone acting on their behalf.

(2) This procedure does not apply to concealed monitoring conducted as part of testing or training exercises when the subjects are participants who have consented to the concealed monitoring as part of an approved testing or training plan. A Defense Intelligence Component may, however, collect, retain, and disseminate USPI in the course of such concealed monitoring only if otherwise authorized by this issuance.

(3) The installation or use of any monitoring device in the United States in circumstances in which a person has a reasonable expectation of privacy, as determined by the General Counsel or legal advisor of the Defense Intelligence Component, and a warrant would be required for law enforcement purposes is electronic surveillance as that term is defined in FISA and subject to Paragraph 3.5.c. The use of a monitoring device in such circumstances against a U.S. person outside the United States is subject to Paragraph 3.5.d.

b. Definition of Terms. For the definitions of "CI," "concealed monitoring," "consent," "DoD facilities," "foreign intelligence," "reasonable expectation of privacy," "United States," "U.S. person," and "USPI," see the Glossary.

c. Procedures. Defense Intelligence Components may conduct concealed monitoring only as follows:

(1) In the United States. Components may conduct concealed monitoring on DoD facilities. Components may conduct concealed monitoring outside DoD facilities after coordination with the Federal Bureau of Investigation (FBI) and in accordance with any applicable agreements with the Department of Justice or the FBI. Monitoring is in the United States if the monitoring device or a subject of the monitoring is located in the United States.

(2) Outside the United States. Components may conduct concealed monitoring outside the United States. Monitoring outside DoD facilities must be coordinated with the Central Intelligence Agency (CIA), and appropriate host country officials in accordance with any applicable status of forces agreement (SOFA) or other international agreement.

(3) Approval for Concealed Monitoring That Occurs in the United States or That Is Directed Against a U.S. Person Outside the United States. Concealed monitoring in the United States or directed against a U.S. person outside the United States may be approved by the Defense Intelligence Component head or a delegee, after consultation with the servicing legal office. The General Counsel or legal advisor of the Defense Intelligence Component will determine whether a person has a reasonable expectation of privacy. For monitoring that occurs outside the United States, the approving official must also consider the laws and policies of the host government and any applicable SOFA. Approval of the concealed monitoring will be based on a determination that all of the following criteria have been met:

(a) There is no reasonable expectation of privacy;

(b) Such monitoring is necessary to conduct an assigned foreign intelligence or CI function;

(c) A trespass will not be necessary to effect the monitoring; and

(d) The monitoring is not subject to Procedure 5.

3.7. PROCEDURE 7. PHYSICAL SEARCHES. *DOES NOT PERTAIN TO NSA/CSS*

a. Scope. This procedure applies to nonconsensual physical searches for intelligence purposes of any person or property in the United States and of U.S. persons or their property outside the United States that are conducted by Defense Intelligence Components or anyone acting on their behalf.

b. Definition of Terms. For definitions of "CI," "consent," "domestic activities," "foreign intelligence," "physical search," "United States," and "U.S. person," see the Glossary.

c. Searches Directed Against Active-Duty Military Personnel.

(1) Limitations. Only CI elements of the Military Services with CI investigative authority may be authorized to conduct physical searches directed against active-duty military personnel for intelligence purposes. The Attorney General or the FISC must approve such searches conducted inside or outside the United States in accordance with Sections 1821-1829, 1881b, 1881c, or 1881d(b) of Title 50, U.S.C.

(2) Authority to Request Searches Under FISA. Only the Secretary of Defense, the Deputy Secretary of Defense, the USD(I&S), or the Secretary or the Under Secretary of a Military Department may seek approval for physical searches described in this paragraph. Applications for court orders will be made through the Attorney General after being cleared by the GC DoD.

(3) Emergency Searches Under FISA. A Defense Intelligence Component head with CI investigative authority or a delegee may request that the GC DoD seek authorization directly from the Attorney General in an emergency, if it is not feasible to submit such a request through an official designated in Paragraph 3.7.c.(2), provided that the appropriate official is notified as soon as possible thereafter.

d. Searches Directed Against Other Persons in the United States.

(1) Limitations. Except for searches directed against active-duty military personnel authorized in accordance with Paragraph 3.7.c., a Defense Intelligence Component may not conduct a physical search of any person or property in the United States for intelligence

purposes. This includes both U.S. and non-U.S. persons. A Component may request the FBI to conduct such a search if both of the following conditions are met:

(a) The search is for an authorized foreign intelligence or CI purpose and, if directed at a U.S. person, the foreign intelligence sought is significant and the search is not being undertaken to obtain information about the domestic activities of any U.S. person.

(b) The search meets the definition of a physical search in FISA, and satisfies the requirements of FISA for such searches.

(2) Authority to Request Searches. Only the Secretary of Defense; the Deputy Secretary of Defense; the USD(I&S); the Secretary or the Under Secretary of a Military Department; the DIRNSA/CHCSS; the Director, Defense Intelligence Agency (DIA); the Director, NGA; or the Director, National Reconnaissance Office (NRO), may seek approval for physical searches in accordance with Paragraph 3.7.d.(1). Applications for court orders will be made through the Attorney General after being cleared by the GC DoD.

(3) Emergencies. A Defense Intelligence Component head may request that the GC DoD ask the FBI to conduct a physical search in accordance with Paragraph 3.7.d.(1) in an emergency if it is not feasible to submit such a request through an official designated in Paragraph 3.7.d.(2), provided that the appropriate official is notified as soon as possible thereafter. The FBI must obtain the authorization of the Attorney General in accordance with FISA.

e. Searches of Other U.S. Persons or Their Property Outside the United States.

(1) Requirements. A Defense Intelligence Component may conduct a physical search of the person or property of a U.S. person outside the United States who is not an active-duty Service member if all of the following conditions are met:

(a) The search is for an authorized foreign intelligence or CI purpose;

(b) The search is appropriately coordinated with the CIA; and

(c) The FISC or the Attorney General has authorized the search in accordance with Paragraph 3.7.e.(3); Sections 1881b, 1881c, or 1881d(b) of Title 50, U.S.C.; or Section 2.5 of E.O. 12333.

(2) Authority to Request Searches. Only the Secretary of Defense; the Deputy Secretary of Defense; the USD(I&S); the Secretary or the Under Secretary of a Military Department; the DIRNSA/CHCSS; the Director, DIA; the Director, NGA; or the Director, NRO may seek approval for physical searches in accordance with Paragraph 3.7.e.(1). Applications for court orders will be made through the Attorney General after being cleared by the GC DoD.

(3) Emergencies. A Defense Intelligence Component may conduct a physical search in accordance with Paragraph 3.7.e.(1) in an emergency with the authorization of the Attorney General. A Defense Intelligence Component head may request that the GC DoD seek such

authorization directly from the Attorney General, if it is not feasible to submit such a request through an official designated in Paragraph 3.7.e.(2), provided that the appropriate official is notified as soon as possible thereafter.

3.8. PROCEDURE 8. SEARCHES OF MAIL AND THE USE OF MAIL COVERS. *DOES NOT PERTAIN TO NSA/CSS*

a. Scope. This procedure governs the physical searches of mail, including the opening or other examination of the content of mail, in the United States and abroad, by a Defense Intelligence Component or anyone acting on its behalf. This procedure also applies to the use of mail covers. A Defense Intelligence Component may only search mail or use a mail cover if such activity is for an authorized foreign intelligence or CI purpose. This procedure does not apply to items transported by a commercial carrier (e.g., Federal Express or the United Parcel Service). Such items are subject to the provisions of Procedure 7.

b. Definition of Terms. For the definitions of "CI," "foreign intelligence," "mail in USPS channels," "mail cover," "physical search," "United States," and "U.S. person," see the Glossary.

c. Searches of Mail.

(1) Mail in the United States. CI elements of the Military Services may search the mail of active-duty military personnel for CI purposes when such mail is in the United States, provided that the element complies with the requirements of Paragraph 3.7.c. If the United States Postal Service (USPS) will conduct the search on behalf of the element, the DoD request for such assistance must comply with Paragraph 3.7.c. For a search of mail in the United States of anyone else, including a non-U.S. person, the FBI must conduct the search in accordance with Paragraph 3.7.d.

(2) Mail Outside the United States. CI elements of the Military Services may search the mail of active-duty military personnel for CI purposes when such mail is outside the United States, provided that the element complies with the requirements of Paragraph 3.7.c. Defense Intelligence Components, after appropriate coordination with host nation authorities, may search mail outside the United States of other U.S. persons or non-U.S. persons, provided that the Component complies with any applicable host nation law, SOFA, or other international agreement, and the requirements of Paragraph 3.7.e , if applicable. If the USPS will conduct the search, the element or Component still must comply with Paragraph 3.7.c or 3.7.e, if applicable.

(3) Compliance with Postal Service Regulations. In addition to complying with the requirements of this procedure, all searches of mail in USPS channels must comply with applicable postal regulations. This applies to mail both in and outside the United States.

d. Mail Covers.

(1) A Defense Intelligence Component may, for foreign intelligence or CI purposes, request the USPS to use a mail cover for mail in USPS channels in accordance with Section 233.3(e)(2) of Title 39, Code of Federal Regulations.

(2) For mail that is in foreign postal channels, a Defense Intelligence Component may request a mail cover for mail that is to or from a U.S. person consistent with appropriate law and procedure of the foreign government and the provisions of any applicable SOFA.

3.9. PROCEDURE 9. PHYSICAL SURVEILLANCE. *DOES NOT PERTAIN TO NSA/CSS*

a. Scope.

(1) This procedure governs physical surveillance of any person inside the United States or any U.S. person outside the United States by a Defense Intelligence Component or anyone acting on their behalf. If anyone acting on behalf of a Defense Intelligence Component is conducting physical surveillance, this procedure applies to any devices such person is operating to observe the subject of the surveillance, and not the provisions of Procedure 6.

(2) This procedure does not apply to physical surveillance conducted as part of testing or training exercises when the subjects are participants in an exercise who have consented to the surveillance as part of an approved testing or training plan. It also does not apply to surveillance detection or counter surveillance activities in which Component personnel must detect and elude foreign physical surveillance. A Component may, however, collect, retain, and disseminate USPI in the course of such surveillance detection or counter surveillance activities only if otherwise authorized by this issuance.

b. Definitions of Terms. For the definitions of "CI," "consent," "Defense Intelligence Component employee," "detail," "foreign intelligence," "physical surveillance," "United States," "U.S. person," and "USPI," see the Glossary.

c. Procedures.

(1) Physical Surveillance in the United States.

(a) U.S. Persons in the United States. Defense Intelligence Components may conduct nonconsensual physical surveillance for a foreign intelligence or CI purpose of any U.S. person in the United States who is a present or former military or civilian employee of a Defense Intelligence Component, a present or former contractor of a Defense Intelligence Component or a present or former employee of such a contractor, an applicant for such employment or contracting, or a Military Service member employed by a non-intelligence element of the military.

(b) Non-U.S. Persons in the United States. Defense Intelligence Components may conduct nonconsensual physical surveillance of a non-U.S. person in the United States for an authorized foreign intelligence or CI purpose.

(c) Coordination With Law Enforcement Agencies and Approval Authority.

1. The Defense Intelligence Component head or a delegee must approve nonconsensual physical surveillance in the United States of persons in the categories identified in Paragraphs 3.9.c.(1)(a) and (b). A Component must coordinate any physical surveillance in the United States with the FBI in accordance with any applicable agreements with the Department of Justice or the FBI and, if appropriate, with other law enforcement agencies, unless the physical surveillance is of an active-duty military person while on a military installation.

2. Defense Intelligence Component employees may only participate in nonconsensual physical surveillance in the United States of U.S. persons other than those in the categories identified in Paragraph 3.9.c.(1)(a), when detailed to the FBI or when operating under FBI authorities.

(d) Participation With the FBI. In addition to physical surveillance conducted in accordance with Paragraphs 3.9.c.(1)(a) and (b), a Defense Intelligence Component head or delegee may approve participation in an authorized FBI foreign intelligence or CI physical surveillance operation in the United States when DoD equities are involved. The FBI must request and authorize such participation in writing.

(2) Physical Surveillance Outside the United States.

(a) Criteria. Defense Intelligence Components may conduct nonconsensual physical surveillance of any U.S. person who is outside the United States for an authorized foreign intelligence or CI purpose.

(b) Limitation on Foreign Intelligence Collection. Physical surveillance of a U.S. person outside of the United States to collect foreign intelligence may be authorized only to obtain significant information that cannot reasonably be acquired by other means.

(c) Required Coordination and Approval Authority. The Defense Intelligence Component head or a delegee may approve nonconsensual physical surveillance outside of the United States of any U.S. person for a foreign intelligence or CI purpose. Physical surveillance outside of the United States, with the exception of physical surveillance on a military installation, must be coordinated with the CIA. The approving official must consider the laws and policies of the host government and any applicable SOFA.

3.10. PROCEDURE 10. UNDISCLOSED PARTICIPATION (UDP) IN ORGANIZATIONS.

a. Scope. This procedure governs the participation by NSA/CSS and anyone, including sources, acting on behalf of NSA/CSS in any organization in the United States or any organization outside the United States that constitutes a U.S. person.

b. Exclusions. This procedure does not apply to:

(1) Personal Participation. Activities conducted within an organization solely for personal purposes (i.e., activities undertaken upon the initiative and at the expense of a person for personal benefit).

(2) Voluntarily Provided Information. Activities conducted within an organization by any person who is already a member of the organization, or who joins on his or her own behalf, and later volunteers information to NSA/CSS not in response to a specific request or NSA/CSS tasking.

(3) Publicly Available Information on the Internet. Collection of publicly available information on the Internet in a way that does not require a person to provide identifying information (such as an email address) as a condition of access and does not involve communication with a human being.

c. Definition of Terms. See the Glossary for definitions of "CI," "collection," "Defense Intelligence Component employee," "domestic activities," "foreign intelligence," "foreign power," "intelligence activities," "organization," "organization in the United States," "organization outside the United States that constitutes a U.S. person," "participation," "publicly available," "undisclosed participation (UDP)," "United States," "U.S. person," and "USPI."

d. General Requirement. Anyone acting on behalf of NSA/CSS may join, become a member of, or otherwise participate in an organization in the United States, or in any organization outside the United States that constitutes a U.S. person, if his or her intelligence affiliation is disclosed to an appropriate official of the organization in accordance with Paragraph 3.10.g. Without such disclosure, the other provisions of this procedure must be applied to authorize UDP.

e. Limitations on UDP.

(1) Lawful Purpose. All UDP must be essential to achieving a lawful foreign intelligence or CI purpose, as determined by DIRNSA/CHCSS or delegee, within the assigned mission of NSA/CSS.

(2) Domestic Activities. UDP may not be authorized for the purpose of collecting information on the domestic activities of U.S. persons.

(3) Coordination. All UDP must be coordinated with FBI, CIA, or any other appropriate agency in accordance with E.O. 12333 and applicable policy and agreements.

(4) UDP for Foreign Intelligence Purposes in the United States. UDP may not be authorized in the United States to collect foreign intelligence from or about a U.S. person, or to collect information necessary to assess a U.S. person as a potential source of assistance to foreign intelligence activities. This limitation does not preclude the collection of information about such persons, when volunteered by sources participating in an organization to which such persons belong, if otherwise permitted by Procedure 2.

(5) Duration of UDP. Authorization to conduct UDP that requires specific approval under this procedure will be limited to the duration of the intelligence activity it is supporting or 12 months, whichever is shorter. If specific approval is required by this procedure, an appropriate official must review and re-approve participation for more than 12 months on an annual basis in accordance with this procedure.

(6) Participation for the Purpose of Influencing the Activities of an Organization or Its Members.

(a) UDP may not be authorized for the purpose of influencing the activities of an organization within the United States, or any organization outside the United States that constitutes a U.S. person, or the members of such organizations who are participating for lawful purposes, unless either:

1. Such participation is undertaken on behalf of the FBI in the course of a lawful investigation, or

2. The organization concerned is composed primarily of individuals who are non-U.S. persons and the organization is reasonably believed to be acting on behalf of a foreign power.

(b) When NSA/CSS desires to engage in UDP for such purposes, it will forward its request through the GC DoD to the USD(I&S) for approval, setting forth the relevant facts justifying such participation and explaining the nature of its contemplated activity.

(c) The prohibition on influencing the activities of an organization's members does not apply to non-U.S. persons who are located outside the United States, provided that the approving authority has considered the possible impact on domestic activities.

f. Required Approvals. Subject to the limitations of Paragraph 3.10.e, UDP may be approved as stated in Paragraphs 3.10.f (1) through (5).

(1) No Specific Approval Required. No specific approval under this procedure is required for the following types of UDP:

(a) Education or Training. Attending a course, meeting, seminar, conference exhibition, trade fair, workshop, symposium or participation in educational or professional organizations for the sole purpose of obtaining training or enhancing professional skills,

knowledge, or capabilities of NSA/CSS employees. Directing or tasking employees to conduct intelligence activities is not authorized under this category of UDP.

(b) Cover Activities. Participation in an organization solely for the purpose of obtaining or renewing membership status in accordance with DoD cover policy. Once membership is acquired, any further activities on behalf of NSA/CSS to maintain or enhance cover require approval in accordance with Paragraphs 3.10.f.(2) or (3).

(c) Published or Posted Information. Participation in an organization whose membership is open to the public solely for the purpose of obtaining information published or posted by the organization or its members and generally available to members. The method of obtaining this information must not involve elicitation.

(d) Public Forums – Employment Affiliation Not Required and No Elicitation of USPI. Participation in meetings, seminars, conferences, exhibitions, trade fairs, workshops, symposiums, or similar events sponsored or conducted by an organization, in person or through technical means (e.g., social networking sites, websites, or forums) provided that all of the following conditions are met:

1. The activity is open to the public;

2. Participation is for the purpose of collecting CI or significant foreign intelligence that is not focused on a specific U.S. person;

3. Providing employment affiliation is not a condition of access; and

4. Participation does not involve the elicitation of USPI.

(e) Foreign Entity. Participation in an organization that is an entity openly acknowledged by a foreign government to be directed or operated by that foreign government or is reasonably believed to be acting on behalf of a foreign power, and the organization is reasonably believed to consist primarily of individuals who are non-U.S. persons.

(2) UDP That May Be Approved by DIRNSA/CHCSS or Delegee. DIRNSA/CHCSS or a delegee may approve the following types of UDP:

(a) Non-U.S. Persons as Sources of Assistance. To collect information necessary to identify and assess a non-U.S. person as a potential source of assistance to foreign intelligence or CI activities.

(b) Public Forums – Employment Affiliation Required or Elicitation of USPI May Be Authorized. Participation in meetings, seminars, conferences, exhibitions, trade fairs, workshops, symposiums, or similar events sponsored or conducted by an organization, in person or through technical means (e.g., social networking sites, websites, or forums), provided that all of the following conditions are met:

1. The activity is open to the public;

2. Participation is for the purpose of collecting CI or significant foreign intelligence that is not focused on a specific U.S. person; and

3. One or both of the following applies:

a. Providing employment affiliation is a condition of access; or

b. Participation may involve the elicitation of USPI.

(c) Cover Activities. Participation in an organization beyond obtaining or renewing membership for the purpose of maintaining or enhancing cover that is approved in accordance with DoD cover policy. Directing or tasking a person acting on behalf of NSA/CSS to collect foreign intelligence or CI from or about the organization or its members requires approval in accordance with Paragraph 3.10.f.(3).

(d) U.S. Person Organizations Outside the United States. Participation in organizations outside the United States that constitute U.S. persons, to collect foreign intelligence or CI outside the United States from or about a non-U.S. person located outside the United States.

(3) UDP That May Be Approved by DIRNSA/CHCSS or a Single Delegee. DIRNSA/CHCSS or a single delegee may approve the following types of UDP:

(a) To collect foreign intelligence outside the United States from or about a specific U.S. person or from or about a specific non-U.S. person in the United States.

(b) To conduct authorized CI activities not addressed in Paragraph 3.10.f.(1) or 3.10.f.(2) in or outside the United States, after required coordination with the FBI or CIA.

(c) To collect information inside the United States necessary to identify a U.S. person as a potential source of assistance to foreign intelligence or CI activities.

(d) To collect information outside the United States necessary to assess a U.S. person as a potential source of assistance to foreign intelligence or CI activities.

(4) Other UDP Approvals. UDP that is not specifically addressed in this procedure may be authorized by the USD(I&S) or DIRNSA/CHCSS with notice to the DoD SIOO.

(5) Standards for Review and Approval. The official approving the UDP pursuant to Paragraphs 3.10.f.(2), (3), or (4) must make all of the following determinations:

(a) The potential benefits to national security from the UDP outweigh any adverse impact on civil liberties or privacy of U.S. persons. A factor in this determination will be

whether NSA/CSS will use appropriate safeguards, including limits on duration and scope of the UDP;

(b) The proposed UDP complies with the requirements of Paragraph 3.10.e; and

(c) The proposed UDP is the least intrusive means feasible and conforms to the requirements of Procedure 2.

g. Disclosure Requirement.

(1) General. Unless the UDP is conducted in accordance with Paragraphs 3.10.e. and f., disclosure of the intelligence affiliation of the person who is acting on behalf of NSA/CSS will be made to an executive officer of the organization in question, or to an official in charge of membership, attendance, or the records of the organization. Such disclosure must be sufficient to apprise the official of the fact of the person's affiliation with NSA/CSS (e.g., by identifying the particular Component where the name of the Component itself reveals the intelligence affiliation or by stating the fact of intelligence affiliation where the name does not reveal the underlying affiliation).

(2) Serving as an Official of the Organization. If the official to whom disclosure would be made is also acting on behalf of NSA/CSS, his or her knowledge alone does not meet the disclosure requirement unless that person is the most senior official within the organization. Where the person is not the most senior official in the organization, disclosure must be made to an additional official with actual or apparent authority to act on behalf of the organization in order for the participation not to be UDP.

(3) Records. NSA/CSS will maintain a written record of any disclosure of intelligence affiliation required by this procedure, including the name and title of the person to whom the disclosure was made.

GLOSSARY

G.1. ACRONYMS.

CI	counterintelligence
CIA	Central Intelligence Agency
DIA	Defense Intelligence Agency

DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DoD SIOO	DoD Senior Intelligence Oversight Official
E.O.	Executive order
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
GC DoD	General Counsel of the Department of Defense
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NSA/CSS	National Security Agency/Central Security Service
NSA OGC	National Security Agency Office of General Counsel
SIGINT	signals intelligence
SOFA	status of forces agreement
TSCM	technical surveillance countermeasures
UDP	undisclosed participation
U.S.C.	United States Code
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USPI	U.S. person information
USPS	United States Postal Service

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

administrative purposes. Information that is received or collected when it is necessary for the administration of a Defense Intelligence Component, but is not received or collected directly for intelligence purposes. Examples include information about systems administration; the performance of contractors; public affairs and legislative matters, including correspondence files; personnel and training records, and training materials.

agent of a foreign power. Any person, including a U.S. person, who:

(1) 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;

(2) 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;

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

(4) 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

(5) Knowingly aids or abets any person in the conduct of activities described in sub-paragraphs (1) - (3) of this definition or knowingly conspires with any person to engage in such activities.

CI. 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.

collection. Information is collected when it is received by a Defense Intelligence Component, whether or not it is retained by the Component for intelligence or other purposes. Collected information includes information obtained or acquired by any means, including information that is volunteered to the Component. Collected information does not include:

Information that only momentarily passes through a computer system of the Component;

Information on the Internet or in an electronic forum or repository outside the Component that is simply viewed or accessed by a Component employee but is not copied, saved, supplemented, or used in some manner;

Information disseminated by other Components or elements of the Intelligence Community; or

Information that is maintained on behalf of another U.S. Government agency and to which the Component does not have access for intelligence purposes.

communications security. A component of cybersecurity that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptographic security, transmission security, emissions security, and physical security of communications security material. Communications security does not include collecting foreign intelligence or CI, or conducting any other intelligence activities.

communications security investigation. An investigation, by an authorized investigative entity, conducted as a result of a communications security incident.

concealed monitoring. The use of hidden electronic, optical, or mechanical devices to monitor a particular person or a group of persons without their consent in a surreptitious manner over a period of time, in circumstances in which such person or persons do not have a reasonable expectation of privacy. Monitoring is surreptitious when it is conducted in a manner designed to keep the subject of the monitoring unaware of it. Video monitoring or sound recording of a subject in a place where he or she has no reasonable expectation of privacy qualifies as concealed monitoring if conducted over a period of time; but taking one photograph of a subject would not qualify. Concealed monitoring does not include electronic surveillance, physical searches, physical surveillance, overhead reconnaissance, or airborne reconnaissance.

consent. An agreement by a person or organization to permit a Defense Intelligence Component to take particular actions affecting that person or organization. Consent should be in written or in electronic form, but may be given orally, unless a specific form of consent is required by law or a particular procedure.

Consent may be implied if adequate notice is provided that a particular action carries with it the presumption of consent to an accompanying action. Consent may also be implied where adequate policy has been published or otherwise articulated.

The General Counsel or legal advisor of a Defense Intelligence Component will determine whether a notice or policy is adequate and lawful, before the Component takes or refrains from taking action on the basis of implied consent.

cooperating sources. Persons or organizations who knowingly and voluntarily provide information, or access to information, at the request of Defense Intelligence Components, or on their own initiative. Cooperating sources include government agencies, law enforcement authorities, credit agencies, commercial entities, academic institutions, employers, and foreign governments.

Defense Intelligence Component employee. A person employed by, assigned or detailed to, or who otherwise conducts intelligence activities on behalf of the Component, except that this term does not include a human source.

Defense Intelligence Components. All DoD organizations that perform foreign intelligence or CI missions or functions, including:

The NSA/CSS.

The DIA.

The NRO.

The NGA.

The foreign intelligence and CI elements of the Active and Reserve Components of the Military Departments, including the United States Coast Guard when operating as a service in the Department of the Navy.

The offices and staff of the Senior Intelligence Officers of the Combatant Command Headquarters.

Other organizations, staffs, and offices, when used for foreign intelligence or CI activities to which Part 2 of E.O. 12333 applies; however, the heads of such organizations, staffs, and offices are not considered Defense Intelligence Component heads for purposes of this issuance. When necessary, DoD policy will establish which official will serve as the Defense Intelligence Component head for these organizations, staffs, or offices.

Defense Intelligence Component head.

The DIRNSA/CHCSS.

The Director, DIA.

The Director, NRO.

The Director, NGA.

The Deputy Chief of Staff, G2, Department of the Army.

The Commander, U.S. Army Intelligence and Security Command.

The Director of Naval Intelligence.

The Director, Naval Intelligence Activity.

The Commander, Office of Naval Intelligence.

The Commander, U.S Fleet Cyber Command.

The Director, Naval Criminal Investigative Service.

The Director of Intelligence, Marine Corps.

The Commander, Marine Corps Intelligence Activity.

The Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance, Department of the Air Force.

The Commander, Twenty Fifth Air Force.

The Commander, Air Force Office of Special Investigations.

The Senior Intelligence Officers of the Combatant Command Headquarters.

Senior officials designated by the Secretary of a Military Department for the foreign intelligence and CI elements of that Department.

Senior officials designated by the USD(I&S) for other Defense Intelligence Components.

detail. A status under which, by agreement between government agencies or elements of the Intelligence Community, an employee of one agency or element operates under the authorities, regulations, policies, and supervision of another.

dissemination. The transmission, communication, sharing, or passing of information outside a Defense Intelligence Component by any means, including oral, electronic, or physical. Dissemination includes providing any access to information in a Component's custody to persons outside the Component.

DoD facilities. Installations or facilities owned, leased, or occupied by accommodation or otherwise, by DoD.

domestic activities. Activities that take place within the United States that do not have a significant connection with either an agent of a foreign power or a foreign power, organization, or person.

electronic surveillance. The acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter. Electronic surveillance is also defined in FISA, and where these procedures reference that definition, FISA should be consulted.

foreign connection. A reasonable belief that the U.S. person is or has been in contact with, or has attempted to contact, a foreign person or a representative or agent of a foreign country, for purposes harmful to the national security interests of the United States; or when a reasonable belief exists that the U.S. person is acting or encouraging others to act in furtherance of the goals or objectives of a foreign person or power, or a representative or agent of a foreign power, for purposes harmful to the national security interests of the United States.

foreign intelligence. Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

foreign power. Any of the following:

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

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

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

A group engaged in international terrorism or activities in preparation thereof.

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

An entity that is directed and controlled by a foreign government or governments.

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

host of a shared repository. An entity responsible for developing and maintaining a shared repository. A host may or may not have access to information in the repository for intelligence purposes.

imagery. A likeness or presentation of any natural or manmade feature or related object or activity and the positional data acquired at the same time the likeness or representation was acquired, including products produced by space-based national intelligence reconnaissance systems and likenesses or presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means. Imagery does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations. This definition is consistent with Section 467 of Title 10, U.S.C.

incidental collection of USPI. Collection of USPI that is not deliberately sought by a Defense Intelligence Component, but that is nonetheless collected. Collection of USPI that is not deliberately sought is considered incidental regardless of whether it is expected or reasonably anticipated to occur.

intelligence. Includes foreign intelligence and CI.

intelligence activities. All activities that the DoD Components conduct pursuant to E.O. 12333.

Intelligence Community and elements of the Intelligence Community.

The Office of the Director of National Intelligence.

The CIA.

The NSA/CSS.

The DIA.

The NGA.

The NRO.

The intelligence and CI elements of the Army, the Navy, the Air Force, and the Marine Corps.

The intelligence elements of the FBI.

The Office of National Security Intelligence of the Drug Enforcement Administration.

The Office of Intelligence and Counterintelligence of the Department of Energy.

The Bureau of Intelligence and Research of the Department of State.

The Office of Intelligence and Analysis of the Department of the Treasury.

The Office of Intelligence and Analysis of the Department of Homeland Security.

The Intelligence and Counterintelligence elements of the Coast Guard.

The other offices with the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.

Such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the Intelligence Community.

intentional collection of USPI. Collection of USPI that is deliberately sought by a Defense Intelligence Component.

international narcotics activities. Activities outside the United States involving the production, transfer, or sale of significant quantities of narcotics or other substances controlled in accordance with Sections 811 and 812 of Title 21, U.S.C., or activities inside the United States that are directly tied to such activities overseas.

international terrorism or international terrorist activities. Activities that 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 within the United States or a State, local, or tribal jurisdiction; appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping; and occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear to be intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

mail cover. The non-consensual recording of any data appearing on the outside cover of any sealed or unsealed mail matter. In this context, a "recording" means a transcription, photograph, photocopy, or other facsimile of the image of the outside cover, envelope, or wrappers of mail matter. A mail cover does not include opening or examination of mail that constitutes a physical search.

mail in USPS channels. Mail while in transit within, among, and between the United States (including mail of foreign origin that is passed by a foreign postal administration to the USPS for forwarding to a foreign postal administration under a postal treaty or convention and mail temporarily in the hands of the U.S. Customs Service or the Department of Agriculture), the Military Postal Service Agency, Army or Air Force Post Offices and Fleet Post Offices, and mail for delivery to the United Nations, New York.

Mail in USPS channels includes international mail in transit to an addressee in the United States after receipt by the USPS from a foreign postal administration or international mail in transit to an addressee abroad before passage to a foreign postal administration.

Mail is in transit until it is physically delivered to the specific addressee in the United States who is named on the envelope or his or her authorized agent.

organization. For purposes of Procedure 10, an organization is an association of two or more individuals formed for any lawful purpose whose existence is formalized in some manner (e.g., by having a defined leadership, holding meetings, publishing a charter, or requiring dues). The term "organization" includes corporations, other commercial entities, and associations formed for a social, political, fraternal, professional, business, academic, ethnic-affinity, or religious purpose, including those that meet and communicate through the use of technologies. The term "organization" does not include a loose group of friends, social contacts, or business associates who may share common interests but whose association lacks any formal structure. For example, the Rotary Club is an organization; a group of friends who play poker or meet at a gym for athletics every weekend is not. A Defense Intelligence Component should consult with the legal

office responsible for advising it if there is any question as to whether a group or an entity constitutes an organization.

organization in the United States. An organization physically located in the United States, whether or not it constitutes a U.S. person. Thus, a branch, subsidiary, or office of an organization in the United States that is physically located outside the United States is not an organization in the United States. Conversely, a branch, subsidiary, or office of a foreign organization, or one substantially made up of foreign persons that is physically located in the United States, is an organization in the United States. An organization in the United States includes an organization that primarily meets and communicates on the Internet or through the use of other technologies and is substantially composed of persons who are located in the United States.

organization outside the United States that constitutes a U.S. person. An organization physically located outside the United States that is substantially composed of U.S. persons. This definition includes an organization that primarily meets and communicates on the Internet or through the use of other technologies and is substantially composed of U.S. persons who are located outside the United States.

overhead reconnaissance. Activities carried out by space-based capabilities whose principal purpose is conducting or enabling imagery collection.

participation. Taking part in an organization's activities and interacting with its members within the structure or framework of the organization. Such activities may include one or more of the following: acquiring membership, attending or taking part in organizational meetings, events, activities, or other forums sponsored or conducted by the organization; conducting the work or functions of the organization; serving as a representative or agent of the organization; or contributing funds to the organization other than in payment for goods or services. Actions taken outside the organizational structure or framework, however, do not constitute participation. Thus, attendance at meetings or social gatherings that involve the organization's members, but are not functions or activities of the organization itself, does not constitute participation.

Participation is "on behalf of" a Defense Intelligence Component when a person is tasked or asked to participate in an organization for the benefit of the Defense Intelligence Component. Such a person may already be a member of the organization or may be asked to join. Actions undertaken for the benefit of the Defense Intelligence Component may include collecting information, identifying potential sources or contacts, or establishing or maintaining cover.

Participation "for the purpose of influencing the activities of an organization or its members" is any action taken with the intention of causing a significant effect on the organization's agenda, course of business, core activities, or future direction. Simply voting or expressing an opinion on these matters as a member generally will not fall within this definition.

A Defense Intelligence Component should consult with the legal office responsible for advising it if there is any question as to whether an activity constitutes participation.

personnel security. The security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information or assignment in sensitive positions.

personnel security investigation. Any investigation required for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the DoD for access to classified information, acceptance or retention in the Military Services, assignment or retention in sensitive duties, or other designated duties requiring such investigation. It also includes investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for a national security position.

physical search. Any intrusion on a person or a person's property or possessions for the purpose of obtaining property, information, or stored electronic data or communications and that would require a warrant for law enforcement purposes. A physical search includes an intrusion that violates a reasonable expectation of privacy or that involves a trespass or otherwise physically occupying private property. It also includes the examination of the interior of property or the scan of a person by technical means. The law in this area is subject to change, and a Defense Intelligence Component should consult with the legal office responsible for advising it on those activities that may constitute a physical search. A physical search does not include:

Examinations of areas that are in plain view and visible to the unaided eye if there is no physical trespass;

Examinations of publicly available information;

Examinations of abandoned property in a public place;

Examinations of government property pursuant to Military Rule of Evidence 314(d), Manual for Courts-Martial; or

Electronic surveillance.

Any intrusion authorized as needed to accomplish lawful electronic surveillance as that term is defined in FISA, conducted in accordance with Procedure 5.

physical surveillance. The deliberate and continuous observation by an employee of a Defense Intelligence Component of a person to track his or her movement or other physical activities while they are occurring, under circumstances in which the person has no reasonable expectation of privacy. An employee of a Defense Intelligence Component may operate enhancement devices (e.g., binoculars or still or full motion cameras) to facilitate a physical surveillance. Physical surveillance does not include casual observation, which is short in duration and not intended to track the movement or other physical activities of a person, and also does not include electronic surveillance, concealed monitoring, physical searches, or overhead reconnaissance.

publicly available information. 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. Publicly available information includes information generally available to persons in a military community even though the military community is not open to the civilian general public.

radio communications hearability survey. The monitoring of radio communications to determine whether a particular radio signal can be received at one or more locations and, if reception is possible, to determine the hearability of reception over time.

reasonable belief. When the facts and circumstances are such that a reasonable person would hold the belief. A reasonable belief must rest on facts and circumstances that can be articulated; hunches or intuitions are not sufficient. A reasonable belief can be based on experience, training, and knowledge of foreign intelligence or CI activities as applied to particular facts and circumstances, and a trained and experienced person might hold a reasonable belief that is sufficient to satisfy these criteria when someone unfamiliar with foreign intelligence or CI activities might not.

reasonable expectation of privacy. The extent to which a person in particular circumstances has a reasonable belief that his or her activities, property, or communications are private. Whether a person's expectations are reasonable is fact-specific, and the law in this area is subject to change. The General Counsel or legal advisor of the Defense Intelligence Component should determine whether a person has a reasonable expectation of privacy.

retention. The maintenance of information in either hard copy or electronic format regardless of how the information was collected or how it was disseminated to a Defense Intelligence Component by another Component or element of the Intelligence Community.

shared repository. A database, environment, or other repository maintained for the use of more than one entity. A database, environment, or other repository that a contractor or other entity maintains for the use of a single Defense Intelligence Component, or those acting on its behalf, is not a shared repository.

TSCM. The use of electronic surveillance equipment, other electronic or mechanical devices, and specialized techniques and measures to determine either the existence and capabilities of unauthorized, hostile, or foreign penetration technologies that are used to obtain unauthorized access to classified and sensitive information, and thereby assist in neutralizing and exploiting such technologies; or the susceptibility of electronic equipment to unlawful electronic surveillance.

transmission media vulnerability survey. The acquisition of radio frequency propagation and its subsequent analysis to determine empirically the vulnerability of the transmission media to interception by foreign intelligence services.

UDP. Participation in any organization in the United States, or any organization outside the United States that is a U.S. person, if the person's intelligence affiliation is not disclosed to an appropriate official of the organization.

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

U.S. person. Includes:

A U.S. citizen.

An alien known by the Defense Intelligence Component concerned to be a permanent resident alien.

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

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.

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 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.

USPI. 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. USPI is not limited to any single category of information or technology. 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 number, and Internet Protocol address information. 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.