

# Central Intelligence Agency Intelligence Activities: Procedures Approved by the Attorney General Pursuant to Executive Order 12333

---

## Table of Contents

Section 1. Introduction and Purpose.....	4
1.1 Intelligence activities are necessary to the national security.....	4
1.2 Congress and the President have directed the CIA to engage in intelligence activities. ....	4
1.3 Executive Order 12333 directs that the CIA collect, retain, and disseminate intelligence information concerning U.S. persons in accordance with Procedures established by the D/CIA and approved by the Attorney General, after consultation with the Director of National Intelligence (DNI). ....	4
1.4 The Attorney General has approved these Procedures.....	5
Section 2. Authorities and Responsibilities.....	6
2.1 Statutory authorities and responsibilities. ....	6
2.2 Authorities and responsibilities under Executive Order 12333. ....	6
2.3 Information concerning United States persons that the CIA may collect, retain, and disseminate....	8
Section 3. Applicability, General Principles, and Additional Requirements .....	10
3.1 Scope.....	10
3.2 Applicability.....	10
3.3 General principles.....	10
3.4 General exceptions. ....	11
3.5 Coordination of collection between the FBI and the CIA. ....	12
3.6 Relationship with NSA Procedures. ....	13
3.7 Obligation to report information to DOJ about potential criminal activity. ....	13
Section 4. Collection.....	14
4.1 Collection techniques.....	14
4.2 Basic collection.....	14
4.3 Standard collection. ....	15
4.4 Special collection.....	16
Section 5. Approval and Documentation Requirements for Bulk and Certain Other Collection Activities .	20
5.1 Scope of documentation requirement. ....	20
5.2 Content of documentation.....	20
5.3 Approving officials.....	21
Section 6. Unevaluated Information.....	22

6.1	Scope of application.....	22
6.2	Exceptional handling: Electronic communications and special circumstances.....	23
6.3	Routine handling: Unevaluated information not subject to exceptional handling.....	24
Section 7.	Retention of Information Concerning U.S. Persons.....	26
Section 8.	Dissemination of Information Concerning U.S. Persons.....	28
8.1	Dissemination inside the Intelligence Community.....	28
8.2	Dissemination outside the Intelligence Community.....	28
Section 9.	Participation in Organizations in the United States.....	31
9.1	Applicability.....	31
9.2	Disclosed participation.....	31
9.3	Undisclosed participation.....	31
Section 10.	Compliance and Oversight Responsibilities.....	34
10.1	Compliance.....	34
10.2	Oversight responsibilities.....	34
Section 11.	Emergencies, Exceptions, and Amendments.....	35
11.1	Emergency exceptions to these Procedures.....	35
11.2	Significant legal interpretations.....	35
11.3	Clerical amendments.....	35
Section 12.	Definitions.....	36
12.1	Agent of a foreign power.....	36
12.2	Bulk collection.....	36
12.3	Collection.....	36
12.4	Communications security investigation.....	36
12.5	Concealed monitoring.....	36
12.6	Consent.....	36
12.7	Counterintelligence.....	36
12.8	Dissemination.....	36
12.9	Electronic surveillance.....	37
12.10	Employee.....	37
12.11	Evaluation or evaluated information.....	37
12.12	Foreign intelligence.....	37
12.13	Foreign power.....	37
12.14	Incidentally acquired information.....	37

12.15	Intelligence Community.....	37
12.16	Personnel security investigation .....	37
12.17	Physical search.....	38
12.18	Physical security investigation.....	38
12.19	Physical surveillance .....	38
12.20	Publicly available .....	38
12.21	Retention.....	39
12.22	Unevaluated information.....	39
12.23	United States.....	39
12.24	United States person.....	39
12.25	U.S. Person Identifying Information (USPII).....	40
12.26	United States postal channels.....	40
Section 13.	Administration and Effective Date.....	41



## **Section 1. Introduction and Purpose**

### **1.1 Intelligence activities are necessary to the national security.**

Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to informed decisionmaking in the areas of national security, national defense, and foreign relations. Collection of such information is a priority objective that the Central Intelligence Agency (CIA) shall pursue in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded. Set forth below are Procedures that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. The United States Government, including the CIA, has a solemn obligation to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by federal law, including in the conduct of intelligence activities.

### **1.2 Congress and the President have directed the CIA to engage in intelligence activities.**

Congress and the President have authorized and directed the Director of the CIA (D/CIA) to conduct intelligence activities through enactment of and amendments to the National Security Act of 1947 and the CIA Act of 1949. The President, through issuance of and amendments to Executive Order 12333, *United States Intelligence Activities*, and other Presidential directives, has given the CIA intelligence-related duties and responsibilities and has placed limitations upon intelligence activities undertaken by the CIA.

### **1.3 Executive Order 12333 directs that the CIA collect, retain, and disseminate intelligence information concerning U.S. persons in accordance with Procedures established by the D/CIA and approved by the Attorney General, after consultation with the Director of National Intelligence (DNI).**

These Procedures reflect the requirements of the National Security Act of 1947, as amended, the CIA Act of 1949, as amended, other applicable laws, and Executive Order 12333, as amended. These Procedures implement portions of Part 2 of that Executive Order, which state, in pertinent part:

- (a) Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned and approved by the Attorney General after consultation with the DNI.
- (b) Elements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned and approved by the Attorney General, after consultation with the DNI. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes.



- (c) The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. The authority delegated pursuant to this paragraph . . . shall be exercised in accordance with [the Foreign Intelligence Surveillance Act of 1978, as amended].
- (d) No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without disclosing such person's intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the Intelligence Community element concerned . . . and approved by the Attorney General, after consultation with the [DNI]. Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee. No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where . . . the organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power.

#### **1.4 The Attorney General has approved these Procedures.**

The D/CIA issued these Procedures after consulting with the DNI and obtaining the approval of the Attorney General. These Procedures supersede prior Procedures addressing the same subject and satisfy the requirements of Section 309 (“Procedures for the Retention of Incidentally Acquired Communications”) of the Intelligence Authorization Act for Fiscal Year 2015.

## **Section 2. Authorities and Responsibilities**

All CIA activities must be related to and consistent with the authorities and responsibilities of the CIA set forth in the National Security Act, the CIA Act, Executive Order 12333, or other applicable provisions of law or Presidential directives.

### **2.1 Statutory authorities and responsibilities.**

According to Section 104A of the National Security Act of 1947, as amended, the D/CIA shall:

- (a) Collect intelligence through human sources and by other appropriate means, except that the D/CIA shall have no police, subpoena, or law enforcement powers or internal security functions;
- (b) Correlate and evaluate intelligence related to the national security and provide appropriate dissemination of such intelligence;
- (c) Provide overall direction for and coordination of the collection of national intelligence outside the United States through human sources by elements of the Intelligence Community authorized to undertake such collection and, in coordination with other departments, agencies, or elements of the United States Government which are authorized to undertake such collection, ensure that the most effective use is made of resources and that appropriate account is taken of the risks to the United States and those involved in such collection; and
- (d) Perform such other functions and duties related to intelligence affecting the national security as the President or the DNI may direct.

According to Section 104 of the National Security Act of 1947, as amended, the function of the CIA is to assist the D/CIA in carrying out these four responsibilities. The D/CIA and CIA employees also exercise authorities and fulfill responsibilities set forth in other federal statutes in accordance with the requirements and limitations of those statutes.

### **2.2 Authorities and responsibilities under Executive Order 12333.**

#### **2.2.1 CIA authorities and responsibilities.**

According to Section 1.7(a) of Executive Order 12333, the CIA shall:

- (a) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence;
- (b) Conduct counterintelligence activities without assuming or performing any internal security functions within the United States;
- (c) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;
- (d) Conduct covert action activities approved by the President;
- (e) Conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations consistent with Section 1.3(b)(4) of Executive Order 12333;

- (f) Under the direction and guidance of the DNI, and in accordance with Section 1.3(b)(4) of Executive Order 12333, coordinate the implementation of intelligence and counterintelligence relationships between elements of the Intelligence Community and the intelligence or security services of foreign governments or international organizations; and
- (g) Perform such other functions and duties related to intelligence as the DNI may direct.

### **2.2.2 Intelligence Community authorities and responsibilities.**

According to Sections 1.3, 1.4, 1.5, and 1.7 of Executive Order 12333, as an element of the Intelligence Community, the CIA shall:

- (a) Serve as the Functional Manager for human intelligence;
- (b) Coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities outside the United States;
- (c) Collect and provide information needed by the President and, in the performance of executive functions, the Vice President, the National Security Council (NSC), the Homeland Security Council, the Chairman of the Joint Chiefs of Staff, senior military commanders, other Executive branch officials and, as appropriate, the Congress of the United States;
- (d) In accordance with priorities set by the President, collect information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;
- (e) Analyze, produce, and disseminate intelligence;
- (f) Conduct administrative, technical, and other support activities within the United States and abroad necessary for the performance of authorized activities, to include providing services of common concern for the Intelligence Community as designated by the DNI;
- (g) Conduct research, development (including testing), and procurement of technical systems and devices relating to authorized functions and missions or the provision of services of common concern for the Intelligence Community;
- (h) Protect the security of intelligence related activities, information, installations, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Intelligence Community elements as are necessary;
- (i) Deconflict, coordinate, and integrate all intelligence activities and other information gathering in accordance with Section 1.3(b)(20) of Executive Order 12333; and
- (j) Perform such other functions and duties related to intelligence activities as the President may direct.



### **2.2.3 Assistance to law enforcement and other civil authorities.**

In accordance with Section 2.6 of Executive Order 12333, the CIA may:

- (a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property, and facilities of any element of the Intelligence Community;
- (b) Unless otherwise precluded by law, such as Section 104A(d)(1) of the National Security Act, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities;
- (c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the General Counsel; and
- (d) Render any other assistance and cooperation to law enforcement or other civil authorities not precluded by applicable law, such as Section 104A(d)(1) of the National Security Act.

### **2.3 Information concerning United States persons that the CIA may collect, retain, and disseminate.**

Section 2.3 of Executive Order 12333 permits collection, retention, and dissemination of information concerning United States persons (U.S. persons). Consistent with that Executive Order, the CIA may collect, retain, and disseminate the following types of information concerning U.S. persons if done in the course of CIA's duly authorized intelligence activities and in fulfillment of the CIA's national security responsibilities:

- (a) Information that is publicly available or collected with the consent of the person concerned;
- (b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by the CIA, provided that no foreign intelligence collection may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;
- (c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug, or international terrorism investigation;
- (d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;
- (e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting;

- (f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;
- (g) Information arising out of a lawful personnel security investigation, physical security investigation, or communications security investigation;
- (h) Information acquired by overhead reconnaissance not directed at specific United States persons;
- (i) Incidentally acquired information that may indicate involvement in activities that may violate federal, state, local, or foreign laws; and
- (j) Information necessary for administrative purposes.

## **Section 3. Applicability, General Principles, and Additional Requirements**

### **3.1 Scope.**

The CIA is responsible for conducting many different types of intelligence activities, primarily focused abroad. Internal CIA regulations govern all of the CIA's intelligence activities. These regulations generally require managerial or higher-level approval and authorization to initiate particular intelligence activities and may impose additional requirements on the conduct of such activities. If duly authorized intelligence activities include collecting information concerning **U.S. persons**, participating in organizations in the **United States**, or other areas governed by these Procedures, then CIA **employees** must also comply with these Procedures.

### **3.2 Applicability.**

These Procedures apply to the intelligence activities of all CIA **employees** (including individuals acting on behalf of the CIA, such as contractors and assets, or persons detailed to the CIA). These Procedures do not apply to CIA **employees** acting solely under the authority of another agency (such as when detailed to another agency) or to the performance of functions and exercise of powers under Section 15 of the CIA Act of 1949, as amended, by CIA **employees** authorized to perform such functions.

**Unevaluated information** is presumed to include **incidentally acquired information** concerning **U.S. persons**, and to be subject to these Procedures regardless of the location of the initial **collection**, unless the CIA obtains specific information to the contrary.

With the exception of Subsection 4.4 ("Special Collection"), nothing in these Procedures shall prohibit **collection, retention, or dissemination** of information concerning **U.S. persons** necessary for administrative purposes, including, but not limited to, contracting, building maintenance, construction, fiscal matters, internal accounting procedures, disciplinary matters, systems administration, public affairs and legislative matters, including correspondence files, personnel and training records, training materials, and investigations of alleged crimes or improprieties by CIA **employees** by CIA components authorized to perform such functions.

Additional legal requirements, such as those imposed by the Freedom of Information Act, the Privacy Act, or the Federal Records Act, may also apply to CIA activities, to **U.S. Person Identifying Information (USPII)**, and to other information concerning **U.S. persons**.

### **3.3 General principles.**

All duly authorized CIA activities subject to these Procedures shall have a purpose consistent with the CIA authorities and responsibilities described in Section 2. In any **collection** activity, the CIA shall collect only the amount of information reasonably necessary to support that purpose.

In accordance with the authorities and responsibilities described in Section 2, CIA uses lawful means to collect intelligence, including open source intelligence. CIA is not authorized to and shall not collect or maintain information concerning **U.S. persons** solely for the purpose of monitoring (1) activities protected by the First Amendment or (2) the lawful exercise of other rights secured by the Constitution or laws of the United States.



In accordance with the authorities and responsibilities described in Section 2, the CIA is not authorized to and shall not engage in any intelligence activity, including **dissemination** of information to the Executive Office of the President, for the purpose of affecting the political process in the United States. Questions about whether a particular activity falls within this prohibition will be resolved in consultation with the Office of General Counsel (OGC).

The CIA shall carry out all activities in accordance with the Constitution and applicable provisions of U.S. statutes, Executive orders, and other Presidential directives. Where appropriate to ensure compliance with these requirements, CIA shall promptly issue an additional implementation guidance document in consultation with the Department of Justice to provide enhanced safeguards beyond those specifically set forth in these Procedures. Such guidance may address, for example, collection and handling of **U.S. person** information that is significant in volume, proportion, or sensitivity, including information in which **U.S. persons** had a reasonable expectation of privacy under the Fourth Amendment of the U.S. Constitution at the time of **collection**. Enhanced safeguards may include measures designed to ensure that the **collection**, handling (including querying), **retention**, and **dissemination** of such **U.S. person** information is lawful and furthers substantial government interests that are within the scope of the CIA's duly authorized activities.

The CIA shall not request any person or entity to undertake any activity that is prohibited by these Procedures, and shall not substantially participate in any such activity. "Substantial participation" means requesting a particular activity or providing technical equipment, funds, or other assistance in support of a particular activity. Therefore, for example, requests to foreign intelligence or security services to conduct **collection** activities, or participation with foreign intelligence or security services in the conduct of such activities, must meet the requirements of these Procedures for **collection** activities. In particular, provision of technical equipment, funds, or other assistance to foreign intelligence or security services in support of special collection techniques directed at a particular **U.S. person** must be treated under these Procedures as if undertaken directly by the CIA.

### **3.4 General exceptions.**

Nothing in these Procedures shall prohibit:

- (a) The return of information storage media, raw intercepts, personal property, or information derived therefrom, to entities of cooperating foreign governments which originally provided the information storage media, raw intercepts, or personal property;
- (b) The forwarding of information storage media, raw intercepts, personal property, or information derived therefrom:
  - a. To other elements of the **Intelligence Community**, so long as all such information storage media, raw intercepts, personal property, or information derived therefrom, are processed in accordance with procedures applicable to the **Intelligence Community** element and approved by the Attorney General; or
  - b. To entities of cooperating foreign governments or to domestic governmental entities outside of the **Intelligence Community**, where such information storage media, raw intercepts, personal property, or information derived therefrom, is not used, knowingly retained, or processed within the CIA, such as when the CIA acts as a mere conduit for information intended solely for another entity.

- (c) The acceptance, storage, and maintenance of information storage media, raw intercepts, personal property, or information derived therefrom, belonging to another agency or department, where that agency or department controls access to all such storage media, intercepts, personal property, or information derived therefrom, for operational or analytic purposes, such as information merely stored on or within CIA-maintained infrastructure, or information for which CIA only provides system support or storage as a service or otherwise maintains only as a service of common concern.

### 3.5 Coordination of collection between the FBI and the CIA.

Under Executive Order 12333, Section 1.3(b)(20), the DNI is responsible for ensuring deconfliction and coordination of intelligence activities through issuance of appropriate policies and procedures. Sections 1.3(b)(20)(A) and (B) instruct that, in accordance with those DNI-issued policies and procedures, the Director of the FBI is responsible for coordination of clandestine collection of foreign intelligence through human sources or human-enabled means and counterintelligence activities inside the United States and the Director of the CIA is responsible for the same outside the United States.

CIA shall coordinate **collection** in the **United States** of **foreign intelligence** and **counterintelligence** with the FBI to the extent required by Executive Order 12333. Such **collection** may also be governed by Intelligence Community Directives, memoranda of understanding, or other governing documents executed among the FBI, the CIA, and the Attorney General.

The CIA may generally cooperate with the FBI, in a manner consistent with these Procedures, to pursue a compatible goal under independent authorities without making or receiving a formal request. However, when the goal is not of interest to one agency or is being pursued under an authority not shared by both agencies (e.g., law enforcement authorities), the CIA should receive from or submit to the FBI a formal request for **collection** assistance (“Community Support Letter”).

The D/CIA or designee shall submit all formal requests for FBI **collection** assistance in writing to the Director of the FBI and shall provide the following information:

- (a) A statement that the assistance is relevant to the responsibilities and authorities of the CIA listed in Section 2;
- (b) A description of the support required or requested, including the target of the **collection** activity and why the **collection** is to be directed at that target;
- (c) The reasons why the FBI, rather than the CIA, should conduct the **collection** activity;
- (d) The manner in which the agencies will coordinate the effort; and
- (e) Any additional approvals and or coordination that would be prudent or required.

Any formal request from the FBI for CIA **collection** assistance should be submitted by the Director of the FBI or designee, should include the same elements, and must be approved by the D/CIA or designee.

The National Security Act prohibits the CIA from exercising police or subpoena powers or engaging in law enforcement or internal security functions. As detailed in Section 2.2.3, Executive Order 12333 permits the CIA to assist law enforcement and other civil authorities in limited circumstances that do not violate this statutory prohibition. Any requests from the FBI (or other law enforcement agency) to assist with a law

enforcement activity must receive careful review prior to approval and will require consideration of applicable CIA regulations.

### **3.6 Relationship with NSA Procedures.**

**Electronic surveillance** conducted by CIA **employees** when they are acting under the direction, authority, and control of the Director of the National Security Agency (NSA) shall be conducted pursuant to Attorney General-approved Department of Defense procedures applicable to the NSA, unless otherwise provided by an agreement that designates the governing Attorney General-approved procedures.

### **3.7 Obligation to report information to DOJ about potential criminal activity.**

Title 28, United States Code, Section 535(b) requires employees of executive branch agencies to expeditiously report to the Attorney General any information, allegation, matter, or complaint received by the agency that relates to violations of federal criminal law involving Government officers and employees.

Section 1.6(b) of Executive Order 12333 requires that Intelligence Community elements “report to the Attorney General possible violations of federal criminal laws by employees and of specified federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department, agency, or establishment concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures.”

To fulfill this obligation, information acquired in the course of the CIA’s authorized activities that indicate possible violations of federal criminal law must be reported to the Department of Justice (DOJ) to the extent required by and in accordance with any memorandum of understanding or other document executed by CIA and DOJ.



## Section 4. Collection

The D/CIA has delegated different authorities to **collect** information to different CIA **employees**, generally via CIA offices and entities. In the course of exercising their respective delegated **collection** authorities, CIA **employees** may direct **collection** at a **U.S. person** only in accordance with this section.

In the course of a duly authorized intelligence activity, the CIA may **collect** information concerning **U.S. persons** by any lawful means, provided that:

- (a) The **collection** relates to a CIA authority and responsibility described in Section 2 (“Authorities and Responsibilities”) and falls within a category described in Subsection 2.3 (“Information concerning **United States persons** that the CIA may collect, retain and disseminate”); and
- (b) The information is collected in a manner authorized by these Procedures.

### 4.1 Collection techniques.

A certain **collection** technique may be used only if a less intrusive technique cannot acquire intelligence of the nature, reliability, and timeliness required. As a rule, basic collection and standard collection techniques are less intrusive than special collection techniques.

As part of authorized **collection** activities, these Procedures permit **collection** that involves **incidentally acquired information** concerning a **U.S. person**, subject to any applicable documentation requirements set forth in Section 5. Such information may be **retained** and **disseminated** only in accordance with these Procedures. Any **incidentally acquired information** that is **unevaluated** must be handled in accordance with Section 6 (“Unevaluated Information”) of these Procedures.

Queries of CIA information repositories are not considered **collection**; rather, those queries examine previously collected information and do not require any additional approval under Section 4. However, queries of **unevaluated information** must comport with the requirements of Section 6 (“**Unevaluated Information**”).

### 4.2 Basic collection.

Basic collection is:

- (a) **Collection of publicly available information** concerning a **U.S. person**;
- (b) **Collection** of information obtained with the **consent** of the subject **U.S. person**;
- (c) Requesting that another U.S. Government agency provide **USPII**, consistent with the providing agency’s procedures, that is necessary or reasonably believed to be necessary to understand or assess related information previously provided by that agency;
- (d) Requesting that another U.S. Government agency provide information to indicate whether a person or entity is a **U.S. person** to permit proper application of the protections of these Procedures and other applicable law.

#### 4.2.1 **Basic collection approval authority.**

Supervisor approvals are not required for a CIA **employee** to conduct basic collection, but such **collection** must be conducted consistent with the authorizations and restrictions of these Procedures.

### **4.3 Standard collection.**

#### **4.3.1 Standard collection techniques.**

Any information **collection** technique directed at a **U.S. person** that is not basic collection or a special collection technique under these Procedures shall be considered a standard collection technique. Standard collection techniques primarily include methods used to collect information from the existing records or knowledge of third parties (such as human sources, other federal agencies, or foreign governments).

Examples of standard collection techniques include, but are not limited to:

- (a) Examining federal, state, local, and tribal records;
- (b) Inquiries of intelligence or security services of foreign governments for information that exists in their files;
- (c) Inquiries of assets or other individuals with whom CIA has a relationship for information they possess, or tasking those individuals to collect the information sought via standard collection techniques;
- (d) Requesting intelligence or security services of the U.S. or foreign governments to use their assets to collect the information sought via standard collection techniques;
- (e) Interviewing individuals who possess the information sought or who may be in a position to supply the information sought;
- (f) Examining records to verify education, employment, residence, credit, financial reputation, or other information in a manner consistent with applicable federal law;
- (g) **Physical surveillance**, including via **concealed monitoring**, with the limitations delineated in Subsection 4.3.2.

#### **4.3.2 Limitations applicable to physical surveillance and concealed monitoring.**

Although a standard collection technique, **physical surveillance** of **U.S. persons** by the CIA is limited by Section 2.4 of Executive Order 12333. In addition, CIA **physical surveillance** of any **U.S. person** within the **United States** may be subject to additional requirements for coordination with the FBI as described in Subsection 3.5.

##### **4.3.2.1 Physical surveillance of a U.S. person within the United States.**

The CIA may request that the FBI conduct **physical surveillance** of a **U.S. person** in the **United States** in accordance with Subsection 3.5. The CIA may directly engage in **physical surveillance** of a **U.S. person** within the **United States** only if the **U.S. person** is a present or former **employee**, a present or former contractor of the CIA, a present or former employee of a CIA contractor, or an applicant for any such employment or contracting.

##### **4.3.2.2 Physical surveillance of a U.S. person abroad.**

The CIA may engage in or direct **physical surveillance** of a **U.S. person** abroad only (1) to collect significant **foreign intelligence** or **counterintelligence** that cannot reasonably be acquired by less intrusive means, or (2) if the **U.S. person** is a present or former **employee**, a present or former contractor of the CIA, a present or former employee of a CIA contractor, or an applicant for any such



employment or contracting. **Physical surveillance** may not be used solely to acquire information about potential sources or contacts. The official approving the activity (in accordance with Subsection 4.3.3) shall ensure that CIA **employees** do not undertake **physical surveillance** beyond a period that is justified by the underlying facts and circumstances.

#### **4.3.2.3 Concealed monitoring.**

The CIA may use **concealed monitoring** as a technique, including as part of the **physical surveillance** described in Subsections 4.3.2.1 and 4.3.2.2, subject to the requirements of those subsections. However, use of some **concealed monitoring** mechanisms, such as certain kinds of monitoring for geolocation purposes, may involve a special collection technique rather than a standard collection technique. The General Counsel must concur in any use of **concealed monitoring** within the **United States** or directed at a **U.S. person**.

#### **4.3.3 Standard collection approval authority.**

A CIA **employee** may use standard collection techniques to conduct **communications security investigations, physical security investigations, or personnel security investigations** without approvals under these Procedures, except that the use of **concealed monitoring** techniques require General Counsel concurrence. Internal CIA regulations may require additional approvals.

In all other cases, use of standard collection techniques directed at a **U.S. person** shall be approved by:

- (a) A Chief of Station, Chief of Installation, or Chief of Base; or
- (b) The Deputy Director of the CIA for Operations (DDO); the Associate Deputy Director of CIA for Operations (ADDO); the Chief or Deputy Chiefs of Operations in a CIA Mission Center; a first, second, or third in command of a DO Division or DO Center; or
- (c) Supervisory personnel who are designated by these officials.

An approving official must document that use of standard collection techniques directed at a **U.S. person** complies with the requirements of this section.

### **4.4 Special collection.**

A special collection technique is one that, under the Fourth Amendment to the U.S. Constitution, would require a warrant if employed inside the **United States** for a law enforcement purpose. Some of these techniques, such as **electronic surveillance** and **physical search**, are described below. Whether other techniques, such as certain forms of real-time geolocation, meet this test depends on a case-by-case analysis of the technique, technology, application, and the current state of the law. If a legal question exists regarding whether a proposed **collection** technique to be directed against a **U.S. person** or to be used inside the **United States** is a special collection technique, it must be presumed to be a special collection technique unless OGC determines otherwise.

#### **4.4.1 Special collection techniques.**

Other than in the circumstances described below, the CIA may not use special collection techniques inside the **United States**. However, the CIA may request that the FBI or another federal agency engage in special collection techniques inside the **United States** in accordance with Subsection 3.5 (“Coordination of collection between the FBI and the CIA”). In accordance with Subsection 2.2.3 (“Assistance to law enforcement and other civil authorities”) CIA may also provide specialized equipment and technical



knowledge to assist another federal department or agency in the conduct by that department or agency of lawful and authorized special collection in the **United States**. Expert personnel may be provided only with the prior approval of the General Counsel when such personnel participate in the **collection** of raw information. Translation assistance, however, may be provided without General Counsel approval if CIA personnel do not participate in the **collection** or **dissemination** of raw information.

Outside the **United States**, the CIA may direct special collection techniques at a **U.S. person** only with the approval of the General Counsel, the D/CIA or designee, the Attorney General, and (where applicable) the Foreign Intelligence Surveillance Court, in accordance with Subsection 4.4.2.

#### **4.4.1.1 Electronic surveillance.**

Outside the **United States**, the CIA may engage in **electronic surveillance** that is directed at a **U.S. person** only with the approvals described in Subsection 4.4.2.

Section 2.4(a) of Executive Order 12333 prohibits the CIA from conducting **electronic surveillance** within the United States except to train personnel in the use of **electronic surveillance** equipment, to test equipment, or to conduct countermeasures to hostile **electronic surveillance** in accordance with Subsections 4.4.3 and 4.4.4.

#### **4.4.1.2 Physical search.**

Whether a **physical search** occurs within or outside the **United States** depends on several factors, including the location of the item being searched and the location where the item came into the CIA's possession. For example, the search of a computer physically located abroad is a search outside of the **United States**, regardless of the location of the CIA **employee** conducting the search.

The CIA may conduct a **physical search** outside the **United States** and directed at a **United States person** only with the approvals listed in Subsection 4.4.2.

The CIA may not conduct a **physical search** within the **United States** of real or personal property, except for searches of personal property of non-**U.S. persons** lawfully in the CIA's possession.

The opening of mail within **United States postal channels** is prohibited. CIA **employees** shall treat all opening of mail inside the **United States** and all opening of mail from or to a **U.S. person** as a **physical search** under these Procedures. Examining the exteriors of physical mail ("mail covers") outside **United States postal channels** or requesting that the FBI or other lawful authorities with FBI concurrence examine mail covers in **United States postal channels** is permitted as a standard collection technique that may be approved under Subsection 4.3.3.

#### **4.4.2 Special collection approval authority.**

Any special collection technique directed at a **U.S. person** outside the **United States** (including a **U.S. person's** property or premises outside the **United States**) must be forwarded through the General Counsel for concurrence and approved by the D/CIA or designee, the Attorney General (as required by Section 2.5 of Executive Order 12333), and where applicable, the Foreign Intelligence Surveillance Court.

An official approving the use of a special collection technique directed at a **U.S. person** outside the **United States** must document in writing that, under existing facts and circumstances, the official has determined that there is probable cause to believe that the person or entity at whom the special collection technique is directed is an **agent of a foreign power**, or an officer or employee of a **foreign power**, and that the information sought is significant **foreign intelligence** or **counterintelligence**.

#### 4.4.3 **Testing and training related to electronic surveillance equipment.**

The CIA may train personnel in the use of **electronic surveillance** equipment and the CIA or its contractors on behalf of CIA may test such equipment inside the **United States** if:

- (a) The testing and training activities do not constitute “electronic surveillance” as defined by the Foreign Intelligence Surveillance Act (FISA);
- (b) The CIA directs the testing and training activities solely at laboratory-generated signals, official government communications (where the CIA obtains **consent**), or at **publicly available information**;
- (c) The CIA undertakes the testing and training activities with **consent**;
- (d) The CIA directs the testing and training activities against live signals environments abroad or environments recorded abroad;
- (e) The CIA undertakes the testing and training activities in the course of countermeasures authorized under Subsection 4.4.4; or
- (f) The CIA conducts such activities in the **United States** in accordance with all of the following requirements:
  - (1) It is not reasonable or not technically feasible to train or test solely as described in paragraphs (a) through (e) above;
  - (2) The activities are limited in extent and duration to those necessary to train personnel in the use of **electronic surveillance** equipment and to determine the capability and performance of that equipment;
  - (3) The training or testing activity does not exceed ninety calendar days; however, the training or testing activity may be renewed if approved pursuant to subparagraph (7);
  - (4) The activities do not intentionally target the communications of a particular person;
  - (5) It is unreasonable to obtain the **consent** of persons incidentally subjected to the surveillance;
  - (6) Information derived from communications intercepted in the course of the activities is not retained or disclosed to any person other than a person directly participating in such activity (such as trainees and their instructors), and any printout or other recording is destroyed before or immediately upon completion of the activity, or, in the case of training, as soon as is reasonably possible;
  - (7) The training or testing is approved in writing by the responsible Head of Directorate or Mission Center or designee with the concurrence of the General Counsel, based on their determinations that the particular training or testing program conforms to these Procedures and is otherwise lawful. No testing of **electronic surveillance** equipment inside the **United States** may exceed ninety calendar days without the prior approval of the Attorney General.

#### 4.4.4 **Countermeasures related to electronic surveillance equipment.**

CIA use of countermeasures, including testing or training as may be necessary for such use, to determine the existence and capability of **electronic surveillance** equipment being used unlawfully in the **United States** is permitted if:

- (a) The countermeasures do not constitute “electronic surveillance” as defined by the FISA; or
- (b) The CIA does not intentionally target the communications of a particular person; it is not reasonable to obtain the **consent** of persons incidentally subjected to the surveillance; CIA limits any **electronic surveillance** in extent and duration to that necessary to determine the existence and capability of such equipment; and any information acquired by such surveillance is used only to protect information, personnel, and facilities from unauthorized surveillance or is disseminated only to appropriate agencies (with appropriate caveats) for law enforcement purposes.

The technical parameters of a communication (such as frequency, modulation, bearing, signal strength, and time of activity) may be retained and used for the purpose of undertaking countermeasures, including necessary testing or training, or for **collection** avoidance purposes.

The CIA may undertake countermeasures only with a written finding by the CIA Director of Security, or designees, that the activity is consistent with this section and is necessary to assure the protection of intelligence sources and methods, CIA facilities, or properly classified national security information.



## Section 5. Approval and Documentation Requirements for Bulk and Certain Other Collection Activities

### 5.1 Scope of documentation requirement.

Regardless of whether approval under Section 4 was required to initiate **collection**, an **employee** shall complete specific documentation for:

- (a) Any **bulk collection** activity; or
- (b) Any other **collection** activity resulting in the acquisition of a quantity of information (including **incidentally acquired information**) that:
  - (1) Exceeds the CIA's capability to evaluate the information promptly for **retention** under the criteria of Section 7; or
  - (2) Under the criteria of Section 7, is determined to qualify for **retention in its entirety** without individualized review of the data contained within the set of collected information.

Documentation must be completed as soon as is practicable, preferably prior to: **collection**; initiation of a program that will collect data on an ongoing basis; or the addition or substantial modification of a data type or source to an already-established platform. Documentation not completed prior to receipt of information shall occur as soon as is practicable after receipt, such as upon transmission to CIA Headquarters after the conclusion of field-based **collection** activity (i.e., field-based personnel may examine, receive, organize, and translate information subject to Subsection 5.1 without first receiving approval or preparing documentation under this section) or upon recognition that the collected information is subject to documentation under this section.

Technical personnel who are processing information subject to this section shall not make the information available for analytic or operational purposes until this documentation has been approved by an official specified in Subsection 5.3. However, in emergency circumstances, technical personnel may make the information immediately available for analytic or operational purposes under the exceptional handling requirements of Subsection 6.2.2 without documentation or approval. Any required documentation must be completed and approved as soon as is practicable.

### 5.2 Content of documentation.

The documentation, which may take different forms for different components, shall include:

- (a) The purpose of the **collection** activity, including a description of why the data is reasonably believed to be relevant to a CIA authority and responsibility listed in Section 2;
- (b) The location of the acquisition, including (when known) details regarding how data provided to CIA by an asset, foreign liaison partner, contractor, or other second party was originally acquired by that party;
- (c) The **collection** technique(s) employed, including any reasonable steps that were or will be taken to limit the information to the smallest separable subset of data containing the information necessary to achieve the purpose of the **collection**. These steps could include

employment of filters or similar technology and should be applied as early as practicable in the course of the **collection** activity;

- (d) A statement meeting the requirements of either (1) or (2) below. If the collected data are sorted into multiple subsets, then each subset must be addressed in a separate statement under this paragraph:
  - (1) That the collected information (or a subset thereof), in its entirety, meets the **retention** criteria of Section 7 without individualized review of the data. This statement must describe why any **USPII**, if it were found in the set of collected information, would meet applicable Section 7 **retention** criteria; or
  - (2) That the collected information (or a subset thereof) will be stored and handled as **unevaluated information** under Section 6. A statement under this paragraph shall state:
    - i. whether such **unevaluated information** is anticipated to include **USPII** that is significant in volume, proportion, or sensitivity; and
    - ii. which set of Section 6 handling and querying requirements (exceptional or routine) will be applied to such **unevaluated information**.
- (e) A description of the CIA office(s) responsible for managing the information and how those offices will implement any applicable handling and querying requirements, such as those required by Section 6.

### **5.3 Approving officials.**

A Chief of Station, Chief of Base, or Chief of Installation; a Deputy Director or Associate Deputy Director of a CIA Directorate; an Assistant Director or Deputy Assistant Director of a CIA Mission Center; and supervisory personnel who are designated by these officials may approve documentation as specified in this section.

## Section 6. Unevaluated Information

The CIA's national security mission may require the storage of **unevaluated information** when it is impracticable, infeasible, or detrimental to the CIA mission to determine promptly whether the information qualifies for **retention** under the criteria of Section 7. The requirements of this section balance the CIA's mission with privacy and civil liberties concerns that may arise from the CIA's possession of this information.

Any **unevaluated information** that results from a CIA **collection** activity must be handled in accordance with this section, regardless of whether approval was required under Section 4 when **collection** occurred.

For purposes of these Procedures, any requirement that information be segregated or separated may be satisfied through either physical or logical separation (i.e., separation through software or other computer logic) of the subject information.

### 6.1 Scope of application.

This section does not apply to:

- (a) Information obtained pursuant to a court order or similar legal process (which would be governed by the procedures relevant to that form of legal process);
- (b) Information obtained pursuant to alternative procedures approved by the Attorney General under Executive Order 12333 or approved by the President;
- (c) Information that has been affirmatively determined to qualify for **retention** under Section 7, including sets of information determined to qualify for **retention** in their entirety, provided that determination has been documented as required by Section 5.2(d)(1);
- (d) Information being processed for potential future operational or analytic use (such as information being prepared for ingestion into an operational or analytic system) provided the information is not available for analytic or operational purposes during processing. Any information that is available for any operational or analytic use must meet the requirements of this section; or
- (e) Information acquired by the CIA for the sole benefit of another **Intelligence Community element** where CIA serves only as a conduit or pass-through entity and does not have operational or analytic access to the dataset. Any information to which CIA has analytic or operational access must meet the requirements of this section.

**Unevaluated information** subject to routine handling requirements may be treated as if subject to exceptional handling requirements based on policy or prudential concerns. An official listed in Subsection 5.3 shall approve application of heightened handling requirements as a matter of policy or prudence. That approval shall be documented in accordance with Section 5.



## **6.2 Exceptional handling: Electronic communications and special circumstances.**

### **6.2.1 Unevaluated information subject to exceptional handling requirements.**

The following categories of **unevaluated information** are subject to the exceptional handling requirements set forth at Subsection 6.2.2:

- (a) Nonpublic telephone or electronic communications (including communications in electronic storage) acquired without the **consent** of a person who is a party to the communication.
- (b) **Unevaluated information** that is anticipated to contain **USPII** that is significant in volume, proportion, or sensitivity, documented in accordance with Subsection 5.2(d)(2) by an official listed in Subsection 5.3.

### **6.2.2 Exceptional handling requirements.**

Protections or enhanced safeguards beyond these exceptional handling requirements, such as additional access approvals or additional training requirements, may be applied as deemed appropriate by an official listed in Subsection 5.3.

#### **6.2.2.1 Storage and access requirements.**

**Unevaluated information** that is subject to exceptional handling requirements shall be segregated from information that is not subject to these requirements. Access shall be limited to CIA **employees** who have completed training in the handling of **unevaluated information** under this subsection. An auditable record of activity shall be maintained, to include access, queries made, and justifications for queries subject to Subsections 6.2.3(b) and (c) below (generally, queries designed to retrieve information concerning **U.S. persons**).

#### **6.2.2.2 Destruction requirements.**

**Unevaluated information** that is subject to exceptional handling requirements shall be destroyed no later than five years after the information has been made available to CIA personnel for operational or analytic use. **Unevaluated information** that is unintelligible, including enciphered or encrypted information or information reasonably believed to have secret meaning, is deemed to be available to CIA **employees** only after the information has been decrypted, decoded, or otherwise rendered intelligible.

The five-year limitation under this subsection may be extended to protect against an imminent threat to human life or upon the approval of the D/CIA (after consultation with the General Counsel and the Privacy and Civil Liberties Officer) based on a written determination that an extended storage period is necessary to protect the national security of the United States. Upon such extension, the D/CIA shall complete any notifications required by statute, Executive Order, or other Presidential directive.

The five-year limitation under this subsection may also be extended when necessary to retain information for technical assurance or compliance purposes (including court orders or litigation obligations) provided such retention has been reported as required by applicable statute or Presidential order. Any **unevaluated information** subject to an extension under this subsection shall be rendered inaccessible for operational or analytic purposes.

**Unevaluated information** received from another element of the **Intelligence Community** must be destroyed no later than the point in time, if any, at which the originating element is required to destroy that information, if such information remains subject to the requirements of this section at that time.

### **6.2.3 Querying of unevaluated information subject to exceptional handling requirements.**

A CIA **employee** may query **unevaluated information** covered by Subsection 6.2.1 only in the following circumstances:

- (a) A query that is not designed to retrieve information concerning a **U.S. person** may be made if the query is reasonably designed to retrieve information related to a duly authorized activity of the CIA.
- (b) A query designed to retrieve information concerning a **U.S. person** may be made if the query is reasonably designed to retrieve information related to a duly authorized activity of the CIA and if the subject **U.S. person** has provided **consent**.
- (c) A query designed to retrieve information concerning a **U.S. person** may be made if the query is reasonably designed to retrieve information related to a duly authorized activity of the CIA and if, to the extent practicable, the query is accompanied by a statement explaining the purpose of the query.

## **6.3 Routine handling: Unevaluated information not subject to exceptional handling.**

### **6.3.1 Information subject to routine handling requirements.**

The following categories of **unevaluated information** are subject to the routine handling requirements set forth at Subsection 6.3.3:

- (a) **Unevaluated information** that is not subject to exceptional handling requirements under Subsection 6.2.1.
- (b) **Unevaluated information** other than nonpublic telephone or electronic communications that is otherwise subject to the exceptional handling requirements of Subsection 6.2.1 and that has been masked or obfuscated in accordance with Subsection 6.3.2.

### **6.3.2 Masking or obfuscating exceptional information to prepare it for routine handling.**

**Unevaluated information** other than nonpublic telephone or electronic communications that would be subject to exceptional handling requirements may be treated instead under routine handling requirements in the following circumstances:

- (a) The **unevaluated information** is stored in such a manner that it cannot be retrieved by reference to **USPII**; or
- (b) Any information that would be **USPII** when correlated with the **unevaluated information** is stored separately.

Any **USPII** that has been stored separately under this subsection is subject to exceptional storage and access requirements and to routine (rather than exceptional) destruction requirements. Such information may be unmasked or otherwise obtained from separate storage only in accordance with the exceptional query requirements of Subsection 6.2.3.

### **6.3.3 Routine handling requirements.**

#### **6.3.3.1 Storage and access requirements.**

**Unevaluated information** subject to routine handling requirements must be segregated from information that is not subject to these requirements. To the extent practicable, an auditable record of activity shall be maintained, which may include access, queries made in accordance with Subsection 6.3.4, and any justifications for queries.

#### **6.3.3.2 Destruction requirements.**

**Unevaluated information** that is subject to routine handling requirements must be destroyed no later than twenty-five years after the information is made available to CIA personnel with access to the relevant information repository.

Unintelligible information, including encrypted or enciphered information or information reasonably believed to have secret meaning, is deemed to be available to CIA personnel only after the information has been decrypted, decoded, or otherwise rendered intelligible.

The storage period limitation under this subsection may be extended with the approval of the D/CIA (after consultation with the General Counsel and the Privacy and Civil Liberties Officer) based on a written determination that an extended storage period is reasonable and necessary to accomplish an authorized mission of the CIA.

**Unevaluated information** received from another **element of the Intelligence Community** must be destroyed no later than the point in time, if any, at which the originating element is required to destroy that information, if such information remains subject to the requirements of this section at that time.

### **6.3.4 Querying of unevaluated information subject to routine handling requirements.**

A CIA **employee** may query **unevaluated information** covered by Subsection 6.3.1 if the query is reasonably designed to retrieve information related to a duly authorized activity of the CIA.



## Section 7. Retention of Information Concerning U.S. Persons

Information concerning **U.S. persons** that has been **evaluated** and determined to meet the criteria of this section may be retained.

The CIA may retain information that has been lawfully collected concerning a **U.S. person** if:

- (a) The information is processed to delete **USPII**. In such cases a generic term that does not identify the **U.S. person** in the context of the information, such as “investor,” may be substituted;
- (b) The information is **publicly available**;
- (c) The information is provided to the U.S. Government with **consent** of the subject **U.S. person**;
- (d) The information concerns only corporations or other commercial organizations and is limited to their identities as manufacturers of equipment and related nomenclature or their locations, as, for example, “Ford Mustang” or “Boeing 737;”
- (e) The information is limited to the use of a name in a descriptive sense without linkage to additional information tied to the referenced **U.S. person**, as, for example, “USS Jimmy Carter,” “Rockefeller Center,” or “Amber Alert;”
- (f) The information relates to a U.S. Government official acting in an official capacity;
- (g) The information is **foreign intelligence**;
- (h) The information is **counterintelligence**;
- (i) The information concerns a **United States person** who is or may be, on the basis of that information or other information known to the CIA:
  - a. an **agent of a foreign power**;
  - b. an officer or employee of a **foreign power**; or
  - c. a person or entity acting for, on behalf of, or in collaboration with a **foreign power**.
- (j) The information concerns the suitability or credibility of potential sources or contacts. If the **U.S. person** concerned is not contacted within a reasonable period of time after **collection** is initiated, or, upon being contacted, refuses or declines to be a source or contact, the information retained should be reduced as far as is practicable, such as to a brief summary indicating that the person was considered as a potential source or contact, the reasons why the person was considered, and the reasons why the person did not become a source or contact. (Any greater amount of information may be retained if it qualifies under any of the other categories in this section.);
- (k) The information is necessary to protect **foreign intelligence** or **counterintelligence** sources or methods from unauthorized disclosure;

- (l) The information concerns **personnel, physical, or communications security**;
- (m) The information is suspected to be enciphered or to contain a secret meaning, or was enciphered or did contain a secret meaning. Information may be retained under this paragraph only for the period of time that is reasonably believed to be necessary for cryptanalytic or traffic analytic purposes;
- (n) The information is necessary for the purposes of oversight, accountability, or redress;
- (o) The information indicates involvement in activities that may violate federal, state, local, tribal or foreign laws and, if federal, may be required to be reported to the Department of Justice (see Subsection 3.7);
- (p) The information is relevant to an administrative, civil, or criminal proceeding or investigation;
- (q) The information is required by law or court order to be retained. Information may be retained under this paragraph only for the period of time required by the pertinent law or court order;
- (r) The information is necessary to protect the safety of any persons or organizations;
- (s) The information concerns a person or activity that poses a threat to any facility or personnel of any element of the **Intelligence Community** or any department containing such an element;
- (t) The information is necessary for the maintenance of technical systems or for data integrity purposes, including for the purpose of mitigating inadvertent or mistaken destruction of information, so long as only personnel who are responsible for technical maintenance have access to the information retained under this paragraph;
- (u) The information is necessary for an administrative function of the CIA (see Subsection 3.2);  
or
- (v) The information is necessary to a lawful activity of the United States, and the General Counsel, in consultation with the Department of Justice, determines that such **retention** is lawful.

If information concerning a **U.S. person** qualifies for **retention** under this section, **USPII** relating to that person may also be retained if the **USPII** is necessary, or if it is reasonably believed that the **USPII** may become necessary, to understand, assess, or act on the information.

Access to and use of retained information concerning **U.S. persons** shall be limited to those persons with appropriate security clearances, access approval, and needs related to duly authorized activities. A CIA **employee** may query retained information if the query is reasonably designed to retrieve information related to a CIA authority and responsibility listed in Section 2.

## Section 8. Dissemination of Information Concerning U.S. Persons

Information concerning a **U.S. person**, including **USPII** and **unevaluated information** subject to these Procedures (see Subsection 3.2), may be shared both inside and outside of the **Intelligence Community** only in accordance with the criteria below. Providing another entity with access to a CIA information repository is **dissemination** for purposes of these Procedures (see “Dissemination” definition at Subsection 12.8).

### 8.1 Dissemination inside the Intelligence Community.

Information concerning a **U.S. person** (including **USPII** and **unevaluated information** subject to these Procedures) may be distributed within the CIA to **employees** and those acting on behalf of the CIA who need to know the information in the course of their duties. Such distribution within the CIA is not **dissemination** under these Procedures.

Information concerning a **U.S. person** (including **USPII** and **unevaluated information** subject to these Procedures) may be disseminated to an appropriate **Intelligence Community** element for purposes of allowing the receiving element to determine whether the information is relevant to its responsibilities and may be retained by that element.

### 8.2 Dissemination outside the Intelligence Community.

To the extent practicable, **USPII** should be removed prior to **dissemination** outside of the **Intelligence Community** unless it is necessary or reasonably believed that the information may become necessary to understand, assess, or act on the information being disseminated.

#### 8.2.1 Dissemination of information concerning U.S. persons that meets the retention criteria of Section 7.

Information concerning a **U.S. person** that has been determined to meet the **retention** requirements of Section 7 may be disseminated outside the **Intelligence Community** to:

- (a) The President, the Vice President, the National Security Council, their staffs, and Chiefs of Mission;
- (b) Executive agencies and military departments that need the information to perform their lawful functions;
- (c) Law enforcement agencies having jurisdiction or responsibility for the investigation or prosecution of activities to which the information relates;
- (d) The Senate Select Committee on Intelligence, the House Permanent Select Committee on Intelligence, the Defense Subcommittee of the Senate Committee on Appropriations, and the Defense Subcommittee of the House Committee on Appropriations, and their staffs, when the information is relevant to their oversight responsibilities; and other members of Congress and their staffs pursuant to procedures determined by the Senate Select Committee on Intelligence or the House Permanent Select Committee on Intelligence, as appropriate;
- (e) Entities of cooperating foreign governments or international or foreign organizations, provided that the receiving entities agree to such further restrictions on use and **dissemination** as may be necessary. **Dissemination** under this paragraph requires the DDO or designee; the Chief of Operations in a CIA Mission Center or DO Division or Center or designee; or a Chief of Station,



Base, or Installation to make a written assessment of the anticipated benefits of disseminating the information and the potential risks (including potential harm to identified individuals) resulting from **dissemination**.

- (f) Other recipients, if the **dissemination** is required by, or in accordance with, an applicable provision of law (including for oversight purposes set forth by law); Executive Order; Presidential directive; NSC directive; policy, memorandum of understanding, or agreement approved by the Attorney General; or court order;
- (g) Other recipients, if **dissemination** is for oversight purposes when there is a determination by the CIA that the **dissemination** will assist these entities in the performance of their oversight functions. Such **dissemination** may be to an Executive branch oversight office.
- (h) Other recipients, if the subject of the information provides prior **consent** in writing;
- (i) Other recipients, if the information is reasonably believed to be necessary to prevent harm or injury;
- (j) Other recipients, if the information is **publicly available**;
- (k) Foreign governments and other foreign entities, via double agents, whether or not the information is classified and without the **consent** of the **U.S. person**, upon a written determination by the DDO or designee that:
  - i. It is not reasonable to obtain the **consent** of the **U.S. person**;
  - ii. Such **dissemination** is consistent with the purported access of the double agent;
  - iii. Such **dissemination** is essential to maintaining the credibility of the double agent;
  - iv. Such **dissemination** either is not compromising, or is necessary to support a significant double agent operation despite the effect such **dissemination** could have on the **U.S. person**; and
  - v. In the case of classified information, the anticipated benefits outweigh the losses.
- (l) Other recipients, with D/CIA or designee approval, Privacy and Civil Liberties Officer concurrence, and General Counsel concurrence (after OGC consultation with the National Security Division of the Department of Justice), if the **dissemination** is necessary to a lawful activity of the United States. **Dissemination** under this paragraph requires a written assessment that the anticipated benefits of disseminating the information outweigh the potential risks resulting from **dissemination** and of whether receiving entities should be subject to further restrictions on use and **dissemination**.

### **8.2.2 Dissemination of unevaluated information.**

**Unevaluated information** may be disseminated outside the **Intelligence Community** to any recipient identified in Subsection 8.2.1, provided that the D/CIA or designee, with PCLO and General Counsel concurrence, provides a written assessment of the anticipated benefits of **dissemination** and the potential risks resulting from **dissemination**, a statement that it is not reasonably possible to accomplish the intended objective by disseminating a lesser amount of information, and a statement that the receiving entity has

provided appropriate assurances regarding their handling of the material with respect to the identified potential risks resulting from **dissemination**.

## Section 9. Participation in Organizations in the United States

In the course of conducting duly authorized intelligence activities, those acting on behalf of the CIA may participate in organizations in the **United States** only in accordance with this section.

### 9.1 Applicability.

This section applies to participation by anyone acting on behalf of the CIA in any organization in the **United States**, such as joining such an organization for purposes of enhancing cover or engaging with non-**U.S. persons** as potential sources of **foreign intelligence**, and implements Section 2.9 of Executive Order 12333. Any undisclosed participation in an organization in the **United States** shall be authorized only if it is essential to achieving lawful purposes that comport with the CIA's authorities and responsibilities as described in Section 2 of these Procedures. Any approval for undisclosed participation granted under prior procedures approved by the Attorney General remains in effect for the time period specified in that approval.

This section does not apply to joining or participating in an organization solely for personal purposes (i.e., activities undertaken on the initiative and at the expense of a person for personal benefit). If there is any question about the nature of the participation or whether the person is acting on behalf of the CIA, the participant should consult with OGC for appropriate guidance. (Internal CIA regulations pertaining to outside activities may govern participation in organizations in the **United States** for personal purposes.)

### 9.2 Disclosed participation.

A person acting on behalf of the CIA may join or otherwise participate in an organization in the **United States** if that person's affiliation with the CIA is disclosed to an official authorized to act on behalf of the organization in relation to the activity in question.

### 9.3 Undisclosed participation.

A person acting on behalf of the CIA may join or otherwise participate in an organization in the **United States** without disclosing his or her CIA affiliation to the organization in the situations and with the approvals listed below. (Additional approvals may be required for interactions with particular individuals within those organizations.)

With the approvals below, and unless otherwise specified, CIA **employees** or persons acting on behalf of the CIA under this section may engage in authorized intelligence activities and may live their authorized cover while participating in the organization. In the course of such participation, CIA **employees** or persons acting on behalf of the CIA may **collect** information concerning **U.S. persons** only in accordance with Section 4 of these Procedures. CIA **employees** may therefore collect **publicly available** or volunteered information concerning **U.S. persons** without additional approvals. Volunteered information is information that has been freely provided to a CIA **employee**. For purposes of this section, the CIA may accept information volunteered by a person who is already a member of or a participant in an organization in the **United States**, or information provided by an organization to its members. If a person voluntarily provides information in response to a question, that information may be treated as volunteered. However, if a person provides information in response to a tasking, that information may not be treated as volunteered.

No undisclosed participation shall be undertaken for the purpose of influencing the activity of the organization or its members except as described in Subsection 9.3.2(g).



### 9.3.1 **Undisclosed participation in general.**

As part of a duly authorized intelligence activity, a person acting on behalf of the CIA may join or otherwise participate in an organization in the **United States** in the following circumstances:

- (a) **Official Establishment of a Foreign Government.** A person acting on behalf of the CIA may join or otherwise participate in an official establishment of a foreign government in the **United States**, such as an embassy, foreign mission, or consulate, without disclosing affiliation and in accordance with applicable law.
- (b) **Public Organizations, Conferences, Forums, Online Sites, and Other Public Venues.** Without disclosing affiliation, a person acting on behalf of the CIA may join or otherwise participate in an organization that is generally open to the public where the organization accepts participants regardless of affiliation and does not require disclosure of affiliation as a condition of attendance or access. This subsection also applies to attendance at any seminar, forum, conference, exhibition, trade fair, workshop, symposium, online forum, or similar event or venue that is generally open to the public.
- (c) **Certain Activities Conducted Via the Internet or Other Electronic Information Networks.** A person acting on behalf of the CIA may view, register for, research, join, or otherwise participate in areas available to the public on or via an electronic information network such as the Internet, provided that access to the website, service, or other online area is accomplished using interfaces made available by the online area to any member of the public, and provided that the area does not require disclosure of affiliation as a condition of access.

### 9.3.2 **Undisclosed participation requiring particular approvals.**

As part of a duly authorized intelligence activity, a person acting on behalf of the CIA may join or otherwise participate in an organization in the **United States** without disclosing her or his CIA affiliation in the circumstances and with the approvals outlined below. Without further approvals required under Section 4 of these Procedures, a person acting on behalf of the CIA and collecting information concerning **U.S. persons** in these circumstances may collect only **publicly available** or volunteered information concerning those **U.S. persons**. (This section applies to participation in organizations in the **United States**. Interactions with particular individuals within those organizations may also be subject to other applicable CIA regulations.)

- (a) **Professional Certification, Training, and Education.** With supervisor approval, and without disclosing CIA affiliation, a person acting on behalf of the CIA may participate in or join educational or professional organizations for the sole purpose of receiving professional certifications necessary to perform duties on behalf of the CIA; enhancing professional skills, knowledge, or capabilities; or otherwise receiving training or education relevant to employment. (Conducting activities for purposes beyond those listed here requires separate approval under this section.)
- (b) **Public Organizations, Conferences, Forums, Online Sites, and Other Public Venues that Require Disclosure of Affiliation.** With supervisor approval, and without disclosing CIA affiliation, a person acting on behalf of the CIA may join or otherwise participate in an organization that is generally open to the public where the organization accepts participants regardless of affiliation but requires disclosure of affiliation as a condition of access or entry. This subsection also applies to attendance at

any seminar, forum, conference, exhibition, trade fair, workshop, symposium, online forum, or similar event or venue that is generally open to the public.

- (c) Venues and Organizations Not Generally Open to the Public for Cover Purposes Only. With the approval of Chief, National Resources Division (C/NR) or Chief, Global Deployment Center (C/GDC), and without disclosing CIA affiliation, a person acting on behalf of the CIA may participate in a meeting, briefing, symposium, private club, trade association, online forum, or similar venue sponsored by an organization that is not generally open to the public for the sole purpose of cover maintenance or enhancement. (Conducting activities for purposes beyond those listed here requires separate approval under this section.)
- (d) International Organizations and Organizations with Foreign National Leadership. With DDO approval, and without disclosing CIA affiliation, persons acting on behalf of the CIA may participate in or join an organization in the **United States** when the organization is an international organization, or when the officials of the organization from whom approval for participation or membership ordinarily would be obtained are non-**U.S. persons**, or have relationships with non-**U.S. persons** that are reasonably believed to create a serious security impediment to approaching any of them. The approval for the organization under this subsection may last up to three years. A three-year organizational approval shall permit a number of different persons acting on behalf of the CIA to participate in the organization over that period of time. Each person joining or participating in the organization must be individually approved to join or to participate by C/NR or C/GDC.
- (e) Requesting Assistance from an Employee or Member of an Organization in the United States. With Deputy Director of the CIA (DD/CIA) approval, persons acting on behalf of the CIA may, without disclosing CIA affiliation to the officials of the organization from whom approval for participation ordinarily would be obtained, ask an employee or member of an organization in the **United States** to engage in authorized intelligence activities. The approval for the organization under this subsection may last up to three years. A three-year organizational approval shall permit a number of different persons acting on behalf of the CIA to request assistance in accordance with this subsection over that period of time. Each person requesting assistance in accordance with this subsection must be individually approved to make requests for assistance by C/NR or C/GDC.
- (f) Joining an Organization in the United States. With D/CIA approval, and General Counsel concurrence, on a case-by-case basis, a person acting on behalf of the CIA may join or participate in an organization in the **United States** without disclosing affiliation in circumstances not falling into categories (a) through (e) above.
- (g) Influencing the Activities of an Organization in the United States or Its Members. With D/CIA approval and General Counsel concurrence, on a case-by-case basis, a person acting on behalf of the CIA may join or participate in an organization without disclosing affiliation for purposes of influencing the activity of the organization or its members, but only if the organization concerned is: (1) composed primarily of individuals who are not **United States persons**; and (2) is reasonably believed to be acting on behalf of a **foreign power**.



## **Section 10. Compliance and Oversight Responsibilities**

### **10.1 Compliance.**

CIA policies and guidance issued to implement these Procedures shall include appropriate measures to facilitate compliance and oversight. CIA information systems will be designed to facilitate auditing of access to and queries of information subject to Sections 6 and 7 of these Procedures. These systems shall be audited periodically by the appropriate oversight entities described below.

### **10.2 Oversight responsibilities.**

#### **10.2.1 Executive Director of the Central Intelligence Agency (EXDIR).**

The EXDIR or designee shall establish guidance for the implementation of these Procedures to include development of training, **employee** use of information subject to these Procedures, establishment of oversight mechanisms (such as periodic audit and review), and other issues as required.

#### **10.2.2 The Office of the Inspector General (OIG).**

As part of the Inspector General's (IG) independent statutory responsibilities, the OIG shall conduct audits, inspections, and investigations of CIA programs and operations to determine compliance with applicable statutes and regulations, including these Procedures.

#### **10.2.3 The Office of General Counsel (OGC).**

The Office of General Counsel shall be responsible for the interpretation of these Procedures, resolve any conflict regarding the application of different provisions of these Procedures, and serve as the primary point of contact with the Department of Justice regarding these Procedures.

#### **10.2.4 Privacy and Civil Liberties Officer (PCLO).**

The Privacy and Civil Liberties Officer shall provide advice and assistance to the EXDIR or designee, and other senior CIA officials regarding privacy and civil liberties concerns in implementing these Procedures and shall serve as the primary point of contact with the Privacy and Civil Liberties Oversight Board regarding these Procedures.

#### **10.2.5 Heads of Directorates, Mission Centers, and Independent Offices.**

Heads of Directorates, Mission Centers, and Independent Offices shall implement these Procedures in coordination with the EXDIR or designee, provide training to personnel who require access in the performance of their duties to information governed by these Procedures, and assist the ExDir or designee, IG, and PCLO in conducting oversight.

#### **10.2.6 CIA Employees.**

CIA personnel are responsible to become familiar with and comply with these Procedures and any implementing guidance, refer any questions concerning the interpretation of these procedures to OGC, use the information that is subject to these procedures only for lawful and authorized purposes, and report activities that may be unlawful or contrary to Executive Order or presidential directive to the appropriate chain of command or to the Inspector General.



## **Section 11. Emergencies, Exceptions, and Amendments**

### **11.1 Emergency exceptions to these Procedures.**

Nothing in these Procedures shall be construed to prohibit the **collection** by standard collection techniques (or by special collection techniques outside the **United States**), or the use, **retention**, or **dissemination** of information concerning any person, if securing any approval that would otherwise be required is not practical and there is a reasonable belief that:

- (1) A person's life or physical safety is in imminent danger, and the information is relevant to the danger or its prevention, reduction, or elimination; or
- (2) The time required to secure prior approval would cause failure or delay in obtaining significant intelligence, and such failure or delay would result in substantial harm to national security. In this circumstance, if the activity involves the use of a special collection technique directed at a **U.S. person**, there must be probable cause to believe that the subject **U.S. person** is a **foreign power**, an **agent of a foreign power**, or an officer or employee of a **foreign power**.

In either circumstance, approval by the most senior official available at the time, up to the official whose approval would otherwise be required for the **collection, retention, use, or dissemination**, should be obtained if time permits. If a standard or special collection technique was directed at a **U.S. person**, the official who must normally approve the **collection** technique under Section 4 must be advised as soon as possible. A special collection technique requiring the approval of the Attorney General 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.

### **11.2 Significant legal interpretations.**

The General Counsel shall consult with the Assistant Attorney General for National Security and the Office of the DNI (ODNI) General Counsel regarding significant legal interpretations of these Procedures.

### **11.3 Clerical amendments.**

While substantive amendments to these Procedures require the approval of the D/CIA and the Attorney General after consultation with the DNI, nonsubstantive or clerical amendments, such as correcting typographical errors, updating organizational titles and cross-references, and providing clarifying examples, require only consultation with the ODNI and approval of the D/CIA or designee, and notice to DOJ.

## **Section 12. Definitions**

### **12.1 Agent of a foreign power**

For purposes of these Procedures, **agent of a foreign power** is defined in the Foreign Intelligence Surveillance Act (50 U.S.C. § 1801(b)).

### **12.2 Bulk collection**

**Bulk collection** means the **collection** of data that, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.).

### **12.3 Collection**

**Collection** means the receipt of information by the CIA for official purposes, whether or not the information is retained, subject to the general exceptions listed in Subsection 3.4 and not including information that has been disseminated by other elements of the **Intelligence Community**.

### **12.4 Communications security investigation**

**Communications Security Investigation** means an investigation that involves inquiries into or surveys of protective measures taken to deny unauthorized persons information derived from communications of the United States Government related to the national security and to ensure the authenticity of such communications.

### **12.5 Concealed monitoring**

**Concealed monitoring** means the use of hidden electronic, optical, or mechanical devices to target a particular person or a group of persons without their **consent** in a surreptitious manner over a period of time, in circumstances in which a person does not have a reasonable expectation of privacy. **Concealed monitoring** does not include the use of such devices solely to restrict **collection** activities for purposes of complying with these Procedures or other applicable law, or for the protection of privacy or civil liberties interests.

### **12.6 Consent**

**Consent** means agreeing to do or to allow something or giving permission for something to happen or to be done. **Consent** may be express or implied. **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 notice has been published or otherwise articulated.

### **12.7 Counterintelligence**

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

### **12.8 Dissemination**

For purposes of these Procedures, **dissemination** means the transmission, communication, sharing, showing, or passing of information outside of the CIA by any means, including by providing another entity with access to a CIA information repository, subject to the general exceptions listed in Subsection 3.4.

## 12.9 Electronic surveillance

*The Foreign Intelligence Surveillance Act includes a separate definition of “electronic surveillance” that must be used for any FISA-authorized collection involving the same. See 50 U.S.C. § 1801(f).*

For activities not covered under the FISA, **electronic surveillance** means the acquisition of a nonpublic communication by electronic interception without the **consent** of a person who is a party to the communication or, in the case of a nonelectronic communication, without the **consent** of a person who is visibly present at the place of communication. **Electronic surveillance** does not include the use of radio direction-finding equipment solely to determine the location of a transmitter or the monitoring of **publicly available information**.

## 12.10 Employee

For purposes of these Procedures, **employee** means a person employed by or acting on behalf of the CIA, including any contractors or assets.

## 12.11 Evaluation or evaluated information

Evaluation means reviewing collected information to determine: whether it relates to an authority and responsibility listed in Section 2; whether it contains any information concerning **U.S. persons**; and whether that information meets **retention** criteria and thus may be retained. This process of evaluating information concerning **U.S. persons** by applying **retention** criteria is often referred to as “minimization.” (See also Section 12.22 “unevaluated information.”)

## 12.12 Foreign intelligence

*The Foreign Intelligence Surveillance Act includes a separate definition of “foreign intelligence information” that must be used for any FISA-authorized collection. See 50 U.S.C. § 1801(e).*

For activities not covered under the FISA, **foreign intelligence** means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

## 12.13 Foreign power

For purposes of these Procedures, **foreign power** is defined in the Foreign Intelligence Surveillance Act (50 U.S.C. § 1801(a)).

## 12.14 Incidentally acquired information

**Incidentally acquired information** means information that is not itself deliberately sought or that concerns individuals who are not the targets of **collection** but that is obtained in the course of activities directed at other authorized subjects.

## 12.15 Intelligence Community

**Intelligence Community** and elements of the **Intelligence Community** refers to those agencies described in Section 3.5(h) of Executive Order 12333, as amended, or their successors.

## 12.16 Personnel security investigation

**Personnel security investigation** means an investigation that involves inquiries into the activities of a person granted access to intelligence or retained in a position with sensitive duties to develop information



pertaining to the suitability, eligibility, and trustworthiness of that individual. These investigations are directed only at present or former CIA **employees**, present or former employees of CIA contractors, applicants for such employment, and other individuals who have been granted or who are being considered for security clearances or approvals and other persons with similar associations (such as resettled defectors and their families).

### **12.17 Physical search**

*The Foreign Intelligence Surveillance Act includes a separate definition of “physical search” that must be used for any FISA-authorized **collection**. See 50 U.S.C. § 1821(5).*

For activities not covered under the FISA, **physical search** means any intrusion on a person or a person’s property or possessions without **consent** that is for the purpose of obtaining property, information, or stored electronic data or communications, and that would require a warrant if done for law enforcement purposes inside the **United States**.

### **12.18 Physical security investigation**

**Physical security investigation** means an investigation that involves inquiries into, or surveys of, the effectiveness of security controls or procedures, including controls established around the perimeter of a facility or with respect to equipment or other property and procedures relating to access to and safe storage and disposal of classified information. **Physical security investigations** include the performance of functions and the exercise of powers by CIA **employees** to protect against unauthorized access, physical damage, or injury, or threats of unauthorized access, physical damage, or injury, to CIA installations, property, or **employees**.

### **12.19 Physical surveillance**

**Physical surveillance** means unconsented following or tracking of one or more persons where such individuals have no reasonable expectation of privacy. Any surreptitious devices employed in the course of **physical surveillance** must be used, however, in accordance with Subsection 4.3.2.3 (**concealed monitoring**).

**Physical surveillance** does not include casual observation, which would be short in duration and narrow in scope, and not intended to track the movement of a person. It also does not include **electronic surveillance** or **physical searches**. **Physical surveillance** does not include overhead reconnaissance not directed at specific **U.S. persons**. Overhead reconnaissance not directed at specific **U.S. persons** includes reconnaissance intended solely for calibration of **collection** means or for comparison of characteristics of physical structures or other real or personal property with similar information collected outside the **United States** for purposes of identifying or interpreting that information.

### **12.20 Publicly available**

**Publicly available** means information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer (but not amounting to **physical surveillance**), 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.

Information is **publicly available** only if it is made available to the CIA under conditions or on terms generally available to the public. For example, certain commercially acquired data may be considered **publicly**

**available** if a non-U.S. government person or corporation could acquire that same data in that same way from that same commercial source; however, other commercial acquisitions of data may be so tailored and specialized for government use, and unavailable to a similarly situated private-sector purchaser, that the data cannot be considered **publicly available**.

Information that is **publicly available** is still considered **publicly available** if the information is provided in filtered or obfuscated form for government use for purposes of complying with these Procedures or other applicable law, or for the protection of privacy or civil liberties interests.

### **12.21 Retention**

Retention means the indefinite maintenance of information concerning **U.S. persons**, subject to the general exceptions listed in Subsection 3.4.

### **12.22 Unevaluated information**

**Unevaluated information** means information that has been collected but not yet reviewed to determine whether it relates to an authority and responsibility listed in Section 2 and whether information concerning **U.S. persons**, if any, qualifies for **retention** under Section 7. Any **collection** activity, whether or not it is **bulk collection**, may produce **unevaluated information**. Because of global mobility and communications networks, **unevaluated information** is generally presumed to contain **incidentally acquired information** concerning **U.S. persons**, regardless of the location of **collection**. (See also Section 12.11 “Evaluation or evaluated information.”)

### **12.23 United States**

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

### **12.24 United States person**

The term **United States person** or **U.S. person** means any of the following:

- (a) A U.S. citizen;
- (b) An alien known by the CIA to be a lawful permanent resident (LPR) (also known as a permanent resident alien). An alien who procures a visa or other documentation by fraud or willful misrepresentation of a material fact is not a lawful permanent resident for purposes of these Procedures;
- (c) An unincorporated association substantially composed of U.S. citizens or lawful permanent residents. “Substantially” must be more than insignificant, but a majority is not required; or
- (d) 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 **United States person**.

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

- (a) A person or entity known to be inside the **United States** is presumed to be a **U.S. person**, unless specific information to the contrary is obtained.

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

### **12.25 U.S. Person Identifying Information (USPII)**

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

**USPII** is a subset of information concerning **U.S. persons**. For purposes of these Procedures, the phrase “information concerning U.S. persons” includes any information concerning a **U.S. person**, whether or not the information is **USPII**.

### **12.26 United States postal channels**

Mail is in **United States postal channels** while in transit within, among, and between the **United States** (including mail of foreign origin which is passed by a foreign postal administration to the United States Postal Service (USPS) for forwarding to a foreign postal administration under a postal treaty or convention and mail temporarily in the hands of the United States 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, N.Y.

Mail in **United States postal channels** also 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.

As a rule, mail shall be considered in such postal channels until the moment it is physically delivered to the specific addressee in the **United States** named on the envelope or the addressee’s authorized agent.



### **Section 13. Administration and Effective Date**

A person who is officially acting in the absence of an official may exercise the powers of that **employee**.

Authority granted to an **employee**, other than the General Counsel, may be exercised by any person who is senior in the **employee's** chain of command.

Authority granted to the General Counsel may be exercised by a Deputy General Counsel or an attorney in the Office of General Counsel designated by the General Counsel or Acting General Counsel.

Any designation of a person to exercise authority explicitly permitted by these Procedures includes the designation of multiple persons to serve simultaneously in that capacity.

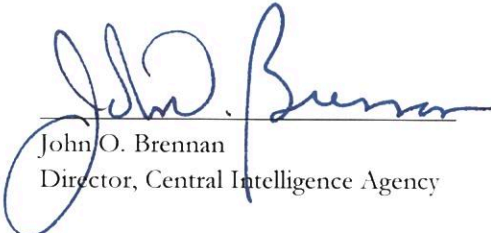
In the event of any changes to organizational structures or titles such that the official title identified in these Procedures no longer exists, approving authority will transfer to the equivalent official under the reorganization.


These Procedures are not intended to, and do not, and may not be relied on to create any substantive or procedural right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

These Procedures shall become effective sixty days after signature by the D/CIA and the Attorney General.

#### **Signatures and Dates Signed**

We approve the foregoing Procedures in accordance with Executive Order 12333, as amended.

  
\_\_\_\_\_  
John O. Brennan  
Director, Central Intelligence Agency

  
\_\_\_\_\_  
Loretta E. Lynch  
Attorney General

10 January 2017  
Date

12 January 2017  
Date