DEPARTMENT OF THE TREASURY

PROCEDURES

FOR

INTELLIGENCE ACTIVITIES

PROCEDURES FOR INTELLIGENCE ACTIVITIES

TABLE OF CONTENTS

INTRODUCTION

These U.S. Department of the Treasury Procedures for Intelligence Activities (Procedures) are established under Section 2.3 of Executive Order (E.O.) 12333, as amended, and are intended to govern all intelligence activities conducted by any component of the U.S. Department of the Treasury (Treasury), including Treasury's element of the Intelligence Community, the Office of Intelligence and Analysis (OIA). These Procedures ensure that Treasury's intelligence activities are carried out in a manner consistent with the constitutional rights of U.S. persons and other protections provided under applicable law and policy. They govern how Treasury and OIA will fulfill their existing responsibilities, and do not confer any new authorities.

I. APPLICABILITY AND SCOPE

A. INTELLIGENCE ACTIVITIES.

These Procedures apply to all intelligence activities conducted by OIA or any other Treasury component in the United States or abroad.[1] These Procedures do not apply to non-intelligence activities that are governed by other executive orders, policies, or procedures and conducted by OIA.

B. COVERED INDIVIDUALS AND COMPONENTS.

1. The Secretary of the Treasury (Secretary), when acting in an intelligence capacity;

2. The Assistant Secretary for Intelligence and Analysis (Assistant Secretary), who serves as the head of OIA;

3. OIA; and

4. Any other Treasury components or employees when they are performing intelligence activities authorized pursuant to E.O. 12333.

II. AUTHORIZED ACTIVITIES AND COORDINATION

A. GENERAL.

OIA shall receive, analyze, collate, and disseminate intelligence and counterintelligence information related to the operations and responsibilities of the entire Department of the Treasury, including all Treasury components and bureaus; collect (overtly or through publicly available sources) foreign financial information and, in consultation with the Department of State, foreign economic information; collect (overtly or through publicly

[1] In these Procedures, "OIA" refers both to the Office of Intelligence and Analysis and, as listed in Section 1.B, other Treasury components and individuals when they are performing intelligence activities.

available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions; and conduct and participate in analytic or information exchanges with foreign partners and international organizations as set forth in E.O. 12333, and other applicable laws, executive orders, Presidential directives, and Intelligence Community Directives (ICDs). These activities include collecting new information and drawing on previously collected information, and are authorized as part of analytic activities or as part of counterintelligence inquiries. In accordance with E.O. 12333 and these Procedures, OIA may collect, retain, and disseminate the following types of information:

1. Publicly available information and information collected with the consent of the person concerned;

2. Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations;

3. Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug, or international terrorism investigation;

4. Information needed to protect the safety of any persons or organizations; including those who are targets, victims, or hostages of international terrorist organizations;

5. Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure and which is information concerning present or former OIA employees, present or former OIA contractors or their employees, or applicants for such employment or contracting;

6. Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;

7. Information arising out of a lawful personnel, physical, or communications security investigation;

8. Information acquired by overhead reconnaissance not directed at specific U.S. persons;

9. Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local, or foreign laws; and

10. Information necessary for administrative purposes.

B. CONDUCT OF ACTIVITIES AND INDIRECT PARTICIPATION.

OIA must carry out all activities in all circumstances in accordance with the Constitution, the laws of the United States, appropriate authorities related to oversight, and applicable

Treasury policy. OIA may not investigate, or collect or retain information about, U.S. persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States. Further, OIA may not participate in or request any person or entity to undertake any activities that are forbidden by E.O. 12333 or these Procedures. In accordance with the authorities and responsibilities described in these Procedures, OIA is not authorized to and will not engage in any intelligence activity, including dissemination of information to the White House, for the purpose of affecting the political process in the United States. Additional guidance regarding the application of this prohibition will be issued as necessary by Treasury after consultation with the Office of the Director of National Intelligence. Questions about whether a particular activity falls within this prohibition will be resolved in consultation with the Treasury's Office of the General Counsel (OGC).

C. COUNTERINTELLIGENCE INQUIRIES.

1. Purpose. OIA may conduct a counterintelligence inquiry to determine the existence of clandestine relationships with foreign powers or organizations, or their agents; contacts with foreign intelligence services; or other hostile activities directed against Treasury facilities, property, personnel, programs, or contractors by foreign powers or organizations, or their agents.

2. U.S. Person Information. As part of a counterintelligence inquiry, OIA may collect U.S. Person Information (USPI) provided that OIA does so in accordance with these Procedures and that any U.S. person about whom OIA is intentionally seeking information falls in one or more of the following categories:

   a. Dual-national visitors and assignees. A U.S. person who also holds citizenship in one or more foreign countries and who is or will be assigned to or visiting a Treasury facility or attending an event sponsored by Treasury or a Treasury contractor. This category includes U.S. persons who have formerly been such visitors or assignees. This category does not include current Treasury employees.

   b. Employees in contact with visitors and assignees. A Treasury employee in contact with a non-U.S. person or dual national who is or will be assigned to or visiting a Treasury facility or attending an event sponsored by Treasury or a Treasury contractor. This category includes a current or former Treasury employee who has previously had contact with such a visitor or assignee.

   c. Employees traveling to foreign countries. A Treasury employee traveling outside the United States and in contact with a non-U.S. person or dual national while outside the United States.

   d. Hostile activities. A Treasury employee or former employee, or any other U.S. person in contact with a Treasury employee or former employee, reasonably

believed to be engaged in international terrorism, unauthorized intelligence collection targeting the United States, or other hostile activities by foreign powers, organizations, or persons, or their agents.

3. Approval and documentation. The Assistant Secretary, or a designee, will approve policy specifying: (i) the level of approval required to initiate and reauthorize a counterintelligence inquiry; (ii) the time period covered by such approvals; (iii) the documentation required for such approvals; and (iv) the documentation required for the use of techniques that may only be used in counterintelligence inquiries.

D. SHARED REPOSITORIES.

OIA may host or participate in a shared repository containing USPI only in accordance with these Procedures and other applicable laws and policies. Each participant in a shared repository must comply with all law, policies, and procedures applicable to the participant for the protection of USPI. Such participants may include Treasury entities other than OIA as well as entities outside Treasury when they participate in a shared repository hosted by OIA.

1. OIA acting as host. OIA acting as a host of a shared repository may perform systems support functions or data-related tasks (*e.g.*, tagging, processing, or marking information) for itself or others. Access to USPI solely for these purposes does not constitute collection, retention, or dissemination under these Procedures. When acting as a host, OIA must enable auditing of access to USPI in a shared repository to the extent practicable.

2. OIA acting as participant. OIA acting as a participant in a shared repository must identify to the host any access and use limitations applicable to the USPI OIA provides. When OIA provides USPI to a shared repository and allows access to or use of the USPI by other participants, OIA has made a dissemination, which it may do only in accordance with section VI below or other applicable Attorney General-approved guidelines. This does not include access to or use of USPI by a host or another element of the Intelligence Community for systems support functions or data-related tasks.

3. Memoranda of Understanding. OIA will also comply with the terms of any authorized Memorandum of Understanding (MOU) that governs OIA's access to shared repositories containing USPI unless OIA's compliance with the terms of any such MOU would violate these Procedures or other Attorney General-approved guidelines.

E. COORDINATION.

OIA will coordinate intelligence activities as follows:

1. Counterintelligence activities in the United States. OIA must coordinate counterintelligence activities in the United States (including the collection of counterintelligence information and the collection of information for the purpose of determining the suitability or credibility of potential sources of counterintelligence information) with the Federal Bureau of Investigation (FBI). In addition, in consultation with OGC:

    a. As soon as an OIA counterintelligence inquiry (including those involving a computer intrusion) reveals a relationship with a foreign intelligence service, OIA must promptly inform the FBI. The FBI will determine whether it will assume responsibility for the matter and/or request that OIA assist the FBI in collecting additional information.

    b. Any indication that classified information may have been disclosed in an unauthorized manner that raises a counterintelligence concern, including disclosure to a foreign power or an agent of a foreign power, must be reported immediately to the FBI. The FBI must be consulted as to all subsequent actions relating to the unauthorized disclosure, and must have timely access to employees and records when it investigates the disclosure.

    c. The Secretary, or a designee, will promptly inform the Attorney General and the Director of National Intelligence (DNI) if Treasury engages in counterintelligence activities in the United States that should have been, but were not, coordinated with the FBI. The Secretary, or a designee, will inform the Attorney General through the FBI, and will also notify the Assistant Attorney General for National Security.

2. Collection of foreign intelligence in the United States. Section 1.7(i) of E.O. 12333 authorizes OIA to collect information, intelligence, and counterintelligence, and Section 1.9 of E.O. 12333 authorizes Treasury, including OIA, to collect foreign financial information and, in consultation with the Department of State, foreign economic information. Collection under these authorities is limited to that which is conducted overtly or through publicly available means. The Secretary, or a designee, will promptly inform the Attorney General and the DNI if Treasury engages in the clandestine collection of foreign intelligence in the United States, which is not authorized under these Procedures. The Secretary, or a designee, will inform the Attorney General through the FBI, and will also notify the Assistant Attorney General for National Security.

3. Compliance with agreements. Treasury will comply with all agreements and MOUs with the Department of Justice, including the FBI, governing the coordination of activities covered by this section.

III. COLLECTION OF USPI

A. INTENTIONAL COLLECTION OF USPI.

OIA may intentionally collect USPI only (i) in accordance with these Procedures, with particular regard to the requirements and limitations in subsections III.D through III.F below; (ii) if the information sought is reasonably believed to be necessary for the performance of an authorized mission or function of OIA; and (iii) if the information falls in one or more of the following categories:

1. Publicly available. The information is publicly available.

2. Overt Collection. OIA also may intentionally collect USPI overtly in the following cases:

   a. Consent. The information concerns a U.S. person who has consented to the collection (*e.g.*, information provided by individuals who consent to computer monitoring in accordance with these Procedures).

   b. Foreign intelligence. The information is reasonably believed to be significant foreign intelligence, the collection is not undertaken for the purpose of acquiring information about any U.S. person's domestic activities (as that term is defined in section XII below), and the U.S. person is one of the following:

      i. An individual reasonably believed to be an officer or employee of, or otherwise acting on behalf of, a foreign power.

      ii. An organization or group reasonably believed to be owned or controlled directly or indirectly by a foreign power.

      iii. An individual, organization, or group reasonably believed to be engaged in or preparing for international terrorist or international narcotics activities.

      iv. An individual, organization, or group reasonably believed to be engaged in or preparing for, on behalf of a foreign power, cyber-enabled attacks on or intrusions into Treasury information systems; Treasury contractors' information systems that impact Treasury personnel, property, or missions; or U.S. Government national security information systems.

v. An individual reasonably believed to be a prisoner of war or missing in action, or who is the target, hostage, or victim of an international terrorist organization.

vi. A person reasonably believed to be acting on behalf of a foreign power, organization, or individual, and to be engaged in activities threatening the national security or economy of the United States.

vii. Corporations or other commercial organizations reasonably believed to be acting for or on behalf of a foreign power, organization, or person engaged in clandestine intelligence activities, sabotage, assassinations, or international terrorist activities.

viii. A person reasonably believed to possess significant foreign intelligence otherwise relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists, which is relevant to the national security or foreign policy, or to the protection against threats to the economy, of the United States.

c. Counterintelligence. The information is reasonably believed to be counterintelligence and the information is acquired as part of properly authorized and conducted analytic activities or a counterintelligence inquiry as described in these Procedures.

d. Current, former, or potential sources of assistance to intelligence activities. The information is about those who are or have been sources of information or assistance, or are reasonably believed to be potential sources of information or assistance, to intelligence activities for the purpose of assessing their suitability or credibility. Information collected for this purpose is limited to publicly available sources, government records checks, and inquiries of Treasury employees. This category does not include investigations undertaken for personnel security purposes.

e. Protection of intelligence sources, methods, and activities. The information is about a person who has access to, had access to, or is otherwise in possession of information that reveals foreign intelligence or counterintelligence sources, methods, or activities, when such collection is reasonably believed necessary to protect against the unauthorized disclosure of such information; provided that the intentional collection of such information will be limited to U.S. persons who fall in one of the following categories:

i. Present or former OIA employees;

ii. Present or former OIA contractors and their employees; or

iii. Applicants seeking employment with OIA or an OIA contractor.

Otherwise, OIA may not collect such information unless done as support to other agencies as described in section VIII below.

f. Threats to safety. The information is needed to protect the safety of Treasury infrastructure, facilities, personnel, programs, contractors, or official visitors, including those who are targets, victims, or hostages of international terrorist activities.

g. Physical security. The information arises out of a lawful physical security investigation.

h. Personnel security investigations. The information arises out of a lawful personnel security investigation. Such USPI may include information contained in personnel files.

i. Communications security. The information arises out of a lawful communications security investigation.

j. Network security. The information is needed for network security, cyber security, and incident response, provided that it otherwise falls into one of the categories in subsections III.A.2.a through III.A.2.i above. Equipment monitoring must also comply with the requirements of subsection IV.C below.

k. Supply chain protection. The information is needed for supply chain risk management efforts, provided that it otherwise falls into one of the categories in subsections III.A.2.a through III.A.2.i above.

l. Other classified and unclassified sensitive information. The information is necessary to protect other classified and unclassified sensitive information, provided that it otherwise falls into one of the categories in subsections III.A.2.a through III.A.2.i above.

m. Overhead reconnaissance. The information is acquired by overhead reconnaissance not directed at specific U.S. persons, provided the collection is authorized in writing by the Assistant Secretary or a designee.

n. Other kinds of information. The information falls in a category other than one of the categories listed above, if approved in accordance with subsection XI.D below.

B. INFORMATION AUTHORIZED BY STATUTE.

OIA is responsible by statute, 31 U.S.C. § 312(b)(2), for "the receipt, analysis, collation, and dissemination of intelligence and counterintelligence information related to the operations and responsibilities of the entire Department of the Treasury." When OIA receives information from other Treasury components pursuant to this statute, OIA may receive the information without regard to its form or volume provided that:

1. OIA's receipt of the information is consistent with OIA's national and departmental missions;

2. The information is otherwise handled in accordance with these Procedures; and

3. OIA has consulted with OGC.

C. INCIDENTALLY COLLECTED OR VOLUNTARILY PROVIDED USPI.

In the course of conducting lawfully authorized activities, OIA may incidentally collect USPI. Entities or individuals may also on their own initiative voluntarily provide information to OIA. All incidentally collected or voluntarily provided USPI is considered "collected" for purposes of these Procedures and may be temporarily retained, evaluated for permanent retention, and disseminated only in accordance with these Procedures. If an entity or individual is voluntarily providing on a recurring basis USPI that OIA could not collect using other provisions of this section, OIA should take appropriate steps to address such collection, consulting with OGC as necessary.

D. COLLECTION INVOLVING SPECIAL CIRCUMSTANCES.

Pursuant to guidance issued by OIA after consultation with OGC and privacy and civil liberties officials, OIA will consider whether collection opportunities require higher-level approval and enhanced safeguards because of the volume, proportion, or sensitivity of the USPI likely to be acquired. When such special circumstances exist, written authorization for the collection must come from the Assistant Secretary, or a designee, after consultation with OGC and OIA's Civil Liberties and Privacy Protection Officer. If advance authorization is not possible, then as soon as practicable after collection begins, the Assistant Secretary, or a designee, must determine in writing, and in consultation with OGC and OIA's Civil Liberties and Privacy Protection Officer, whether to authorize the continued retention of the information in accordance with these Procedures and whether enhanced safeguards would be appropriate. The determination will be based on the following:

1. Proper collection. The information has been or will be properly collected in accordance with these Procedures; and

2. Reasonable under the circumstances. The collection activity is reasonable based on all the circumstances, including the value of the information; the impact and duration of the collection activity, and the resources utilized to conduct that collection activity; the collection methods used by OIA or others; the amount of USPI; the nature and sensitivity of the USPI; the potential for substantial harm, embarrassment, inconvenience, or unfairness to U.S. persons if the USPI is improperly used or disclosed; and the safeguards that will be applied to the information pursuant to these Procedures, including under subsection V.I below.

OIA will provide a copy of all such written authorizations and determinations to OIA's Civil Liberties and Privacy Protection Officer and OGC, and to other officials as needed. In addressing questions about the implementation of this provision, OIA will consult with OIA's Civil Liberties and Privacy Protection Officer and OGC, and with other officials as needed.

E. LEAST INTRUSIVE MEANS.

OIA will use the least intrusive collection techniques feasible within the United States or against a U.S. person abroad. In making this determination, OIA should use the least intrusive technique—considering the privacy and civil liberties of U.S. persons and any potential damage to their reputation—that will also be operationally sound and effective. It is recognized that the choice is a matter of judgment, and this requirement is not intended to discourage OIA from seeking needed intelligence.

F. AMOUNT OF INFORMATION COLLECTED.

In collecting non-publicly available information concerning U.S. persons, OIA will, to the extent practicable, collect the smallest amount of information that meets the requirements of its intelligence mission. This requirement is in addition to the requirement to use the least intrusive collection techniques feasible set forth in subsection III.E above.

IV. COLLECTION TECHNIQUES

A. GENERAL.

OIA may use the techniques authorized in this section to collect information. All activities must conform to the requirements of Section II above, including its coordination requirements, and all collection of USPI must conform to the requirements of Section III above. In accordance with Sections 1.7(i) and 1.9 of E.O. 12333, OIA may only collect information overtly or through publicly available sources. This limitation applies to any technique used, whether inside or outside the United States. OIA does not have authority to engage in electronic surveillance, unconsented physical searches, mail surveillance, or other techniques where a warrant would be required for law enforcement purposes. If OIA believes that there is a need to use such a technique, it should consult

with OGC and consider referring the matter to another IC element or law enforcement entity with the appropriate authority.

B. AUTHORIZED TECHNIQUES.

1. Analytic activities. To conduct authorized analytic activities, OIA may use the following techniques:

   a. Access and examine publicly available information, Treasury records, and records maintained by other federal, state, local, tribal, or foreign governmental entities or agencies to determine if the information meets the standard for collection.

   b. Collect publicly available information, including information from online services and resources.

   c. Collect Treasury records and obtain information from Treasury personnel.

   d. Collect records maintained by and information from other federal, state, local, tribal, or foreign governmental entities or agencies, consistent with applicable law, regulation, policy, or agreement.

   e. Interview or request information from members of the public and private entities who are not known to be a witness in, or a subject of, a law enforcement investigation or a counterintelligence inquiry.

   f. Conduct equipment monitoring in accordance with subsection IV.C below.

2. Counterintelligence inquiries. As part of an authorized counterintelligence inquiry, OIA may use the following techniques:

   a. All techniques described in subsection IV.B.1 above.

   b. Witness interviews.

   c. Subject interviews.

   d. Assistance to law enforcement and other civil authorities in accordance with these Procedures.

   e. Consensual physical searches in accordance with subsection IV.D below.

C. EQUIPMENT MONITORING.

1. General. The Assistant Secretary will promulgate a policy to govern the monitoring of computer equipment and telephones by OIA for the purposes described herein.

Any such monitoring by OIA must be done in accordance with the policy, and be consistent with these Procedures, applicable law, and other Treasury policy.

2. Treasury equipment. Any monitoring of Treasury equipment must be done with users' consent and proper notification to users that their communications and activities will be monitored. The Treasury entity responsible for or operating the monitored equipment will require periodic acknowledgements by users that their use of the equipment constitutes consent to monitoring. (Such acknowledgements may be in electronic form.) In order to ensure that, in all circumstances, the means employed to obtain users' consent and provide proper notice are sufficient, the Treasury entity may also:

    a. Place decals on devices being monitored and/or use electronic banner notices on device screens.

    b. Require user agreements acknowledging that monitoring may occur and the use that the Government may make of any information on or obtained from the equipment.

    c. Issue specific memoranda to users or standing operating procedures and instructions.

    d. Conduct workplace training that specifically addresses terms of monitoring.

3. Other equipment. OIA may monitor other equipment, not covered by subsection IV.C.2 above, or obtain the results of such monitoring, when such equipment is present on Treasury sites, locations, or facilities or is connected to Treasury systems. Any such monitoring requires the consent of the users subject to the monitoring and must comply with relevant statutory and constitutional provisions. Before the start of the monitoring and periodically thereafter, OGC must make a written finding that sufficient measures, including those required by subsection IV.C.2 above, establish that the individuals or entities subject to the monitoring have consented to it. In making this finding, OGC may rely on reasonable factual representations made by an outside entity as to the content of banners on the monitored equipment, the details of notices, signs, and user agreements, and similar matters relating to how the entity provides notice to and obtains consent from individuals or entities whose communications or information are monitored.

4. Exclusion. This subsection does not limit Treasury's ability to obtain from another government agency information the other agency has lawfully acquired under its electronic surveillance or other authorities.

D. CONSENSUAL PHYSICAL SEARCHES.

OIA may conduct a consensual physical search of any office space, furniture, or personal items, including desks, filing cabinets, briefcases, and other storage containers, that (i) is within a Treasury facility and (ii) is used by a subject of a counterintelligence inquiry, provided that an inquiry is open pursuant to subsection II.C and:

1. The subject of the inquiry is:

   a. A non-U.S. person; or

   b. A U.S. person who is a present or former employee of Treasury; or

   c. An applicant for employment with Treasury;

2. The subject of the inquiry (or any other person whose office space, furniture, or personal items is being searched) has consented to the search, and OGC has determined that the appropriate consent has been lawfully obtained and that there is a reasonable basis to conclude that the search may return material or other information relevant to the underlying counterintelligence inquiry; and

3. OIA has coordinated the search in accordance with subsection II.E above, as appropriate.

E. OTHER TECHNIQUES.

OIA may use any technique not specifically covered in this section with the written approval of the Assistant Secretary after consultation with OGC, provided that use of the technique is consistent with the limitations in subsection IV.A above and E.O. 12333.

V. RETENTION OF USPI

A. APPLICABILITY.

This section governs OIA's retention of non-publicly available USPI collected without the consent of the person whom the USPI concerns. Information that does not fall within the definition of collection because it was disseminated by another element of the IC is governed by subsections V.C through V.G below.

B. EVALUATION OF INFORMATION.

OIA will evaluate collected information that may contain USPI to determine whether it may be permanently retained under these Procedures, as follows:

1. Intentional collection of USPI. If OIA intentionally collects USPI, whether inside or outside the United States, OIA will evaluate the information promptly. If necessary, OIA may retain the information for evaluation for up to five years. The Assistant Secretary may approve an extended period in accordance with subsection V.B.5 below.

2. Incidental collection of USPI. If, as part of OIA's lawfully authorized activities, OIA incidentally collects USPI, OIA may retain the incidentally collected USPI for evaluation for up to five years. The Assistant Secretary may approve an extended period in accordance with paragraph V.B.5 below. Intentionally collected USPI is subject to subsection V.B.1 above, and information obtained from a special circumstances collection is subject to subsection V.B.4 below, and not this paragraph.

3. Voluntarily provided USPI. If OIA receives information that is voluntarily provided about a person reasonably believed to be a U.S. person, OIA will evaluate the information promptly. If necessary, OIA may retain the information for evaluation for up to five years. The Assistant Secretary may approve an extended period in accordance with subsection V.B.5 below. If OIA receives information that is voluntarily provided about a person reasonably believed to be a non-U.S. person, but the information may contain USPI, OIA may retain the information for evaluation for up to five years.

4. Special circumstances. If OIA conducts a special circumstances collection pursuant to subsection III.D, OIA may retain the information for evaluation for up to five years or for such shorter time approved by the authorizing official. The Assistant Secretary may approve an extended period in accordance with subsection V.B.5 below.

5. Extended retention. The Assistant Secretary may approve, either at the time of collection or thereafter, the further retention of specific information or categories of information subject to subsections V.B.1 through V.B.4 above for no more than five years beyond the time permitted in those subsections. The Assistant Secretary must document the following findings in writing:

   a. The extension is necessary to carry out an authorized mission of OIA; and

   b. OIA will retain and handle the information in a manner consistent with the protection of privacy and civil liberties.

   In making this finding, the Assistant Secretary must also consider the need for enhanced protections, such as those described in subsection V.I below, and consult with OGC and OIA's Civil Liberties and Privacy Protection Officer.

   Any further extension of temporary retention beyond the time specified in this subsection requires an amendment to these Procedures. (See subsection XI.E below.)

6. Unintelligible information. For any information that is not in an intelligible form, the time periods identified above begin when the information is processed into intelligible form. Unintelligible information includes information that OIA cannot decrypt or understand in the original format. To the extent practicable, unintelligible information will be processed into an intelligible form.

C. DELETION OF INFORMATION.

Unless OIA determines that the information covered by subsections V.B.1 through V.B.5 above meets the standards for permanent retention during the specified time period, all USPI (including any information that may contain USPI) must be deleted from OIA's automated systems and all paper files destroyed by the end of the applicable retention period.

D. SHARED REPOSITORIES.

Retention time of USPI received by OIA through a shared repository maintained by an entity other than OIA shall be determined by the entity maintaining the shared repository. The retention periods provided for in this section will, however, apply to any data that OIA copies or extracts by any means from the shared repository.

E. INFORMATION DISSEMINATED BY ANOTHER IC ELEMENT.

If another element of the IC disseminates unevaluated information that may contain USPI to OIA, OIA may only retain the information and evaluate it for permanent retention under subsection V.G below for as long as the originating IC element may retain it, if that period is reported by the originating IC element or can be determined by technical reference, or otherwise for a reasonable period not to exceed 5 years. If the disseminating IC element has already determined that the information meets the disseminating IC element's Attorney General-approved standards for permanent retention, then, as the recipient, OIA must only verify that the information is reasonably believed to be necessary for the performance of OIA's authorized intelligence mission in order to retain the information permanently.

F. INFORMATION OBTAINED UNDER MEMORANDUM OF AGREEMENT.

The retention of information maintained by another entity and obtained or accessed by OIA pursuant to an MOU or other arrangement that is more restrictive than these Procedures is subject to the terms negotiated under that agreement or arrangement in addition to these Procedures.

G. PERMANENT RETENTION.[2]

1. Retention standard. OIA may permanently retain USPI if the USPI is publicly available, collected with the consent of the U.S. person(s) whom the USPI concerns, or a specific determination is made that the USPI falls into one or more of the following categories:

   a. The information was lawfully collected or disseminated to OIA by another element of the IC, and determined at the time of collection or subsequently during temporary retention to meet the collection criteria described in subsection III.A.2 above;

   b. The information was collected incidentally to authorized collection, or disseminated to OIA by another element of the IC, and is necessary to understand or assess the importance of foreign intelligence or counterintelligence, such as information about a U.S. person that provides important background or context for foreign intelligence or counterintelligence;

   c. The information is retained for purposes of oversight, accountability, or redress. OIA will promptly delete information that is retained under this paragraph beyond the period permitted by subsection V.B above once it no longer needs the information for purposes of oversight, accountability, or redress;

   d. The information is imagery collected for a non-intelligence purpose that contains foreign intelligence or counterintelligence information; or

   e. Retention of the information is required by law or by policy approved by the Attorney General, but only for so long as such retention is required by such law or policy.

2. Retention of specific USPI. OIA will determine whether information that contains USPI meets the standard for permanent retention at the most specific level of information that is appropriate and practicable.

H. SPECIAL REQUIREMENTS FOR "COVERED COMMUNICATIONS."

1. Definitions. For purposes of this subsection, as defined in Section 309(a)(1) of the Intelligence Authorization Act for Fiscal Year 2015 (codified at 50 U.S.C. § 1813) (Act), a "covered communication" is any nonpublic telephone or electronic communication acquired without the consent of a person who is a party to the

[2] For purposes of these Procedures, "permanent retention" does not mean that the information is retained indefinitely, but rather that it is retained in accordance with Treasury's applicable records retention policies.

communication, including communications in electronic storage, and "U.S. person" has the meaning given that term in 50 U.S.C. § 1801(i).

2. Limitation on extended retention. If OIA acquires a covered communication as part of an intelligence collection activity not otherwise authorized by court order, subpoena, or similar legal process that is reasonably anticipated to result in the collection of such a communication to or from a U.S. person, OIA may only retain the covered communication for more than five years if:

   a. The communication satisfies the requirements of one or more of the categories identified in section 309(b)(3)(B) of the Act; and

   b. OIA complies with any applicable approval and congressional reporting requirements.[3]

3. Relationship to other provisions. Subsections V.B through V.G above do not apply to covered communications subject to this subsection V.H.

I. ENHANCED SAFEGUARDS.

1. Need for enhanced safeguards. Whenever there is a collection involving special circumstances under these Procedures, the Assistant Secretary, or a designee, in consultation with OGC and OIA's Civil Liberties and Privacy Protection Officer, will assess whether there is a need for enhanced safeguards to protect USPI. This assessment will be made in writing and will consider:

   a. The intrusiveness of the methods used by OIA or others to acquire the USPI.

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

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

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

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

[3] It is also possible that another element of the IC may disseminate a covered communication to OIA where OIA has reason to believe that the disseminating element has not made a determination that the information may be retained in excess of five years in accordance with its section 309 procedures. The provisions of this subsection also apply to such a communication, with the five-year period beginning at the time when the other IC element first collected the communication.

f. Practical and technical difficulties associated with implementing any special safeguards.

g. Any legal or policy restrictions that apply to the data, including the Privacy Act of 1974.

h. Other factors as directed by the Assistant Secretary.

2. Implementation of enhanced safeguards. If the Assistant Secretary, or a designee, determines that there is a need for enhanced safeguards, that official will consider, and identify in writing for implementation, any of the following protections as deemed appropriate:

a. Procedures for review, approval, or auditing of any access or search.

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

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

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

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

f. Additional training requirements.

g. Additional protective retention measures.

J. MAINTENANCE AND DISPOSITION OF INFORMATION.

The maintenance and disposition of USPI that is retained in the automated systems and all paper files of OIA will conform to this section and to OIA records management schedules approved by the Archivist of the United States for the files or records in which the information is retained.

K. RETENTION FOR BACKUP PURPOSES.

Notwithstanding the other provisions of this section (other than the requirements of subsection H with respect to "covered communications"), OIA may retain, process, and query information retained for backup purposes, provided that only personnel responsible

for maintaining and administering such information have access to it. If OIA uses information retained for backup purposes to restore lost, destroyed, or inaccessible information, the other provisions of this section will apply to such restored information.

VI. DISSEMINATION OF USPI

A. APPLICABILITY AND SCOPE.

This section governs the dissemination of USPI outside OIA. Information may be disseminated under this section only if it was properly handled under these Procedures (*e.g.*, properly collected and retained). Within OIA, access to USPI will be limited to those who need the information to perform an authorized function. This section applies to USPI in any form, including automated systems and all paper files and information OIA places in databases or on web sites or shared repositories accessible to other persons or organizations outside OIA. This section does not apply to information disseminated under other procedures approved by the Attorney General or a court order that otherwise imposes controls on such dissemination.

B. CONSISTENCY WITH OTHER LAWS.

All disseminations under this section must be permissible under the Privacy Act of 1974, 5 U.S.C. § 552a, and other applicable laws, and permitted by any enhanced safeguards implemented pursuant to these Procedures.

C. NOTICE TO COMPONENTS.

Before disseminating information obtained from another component of the Treasury Department, OIA will notify the component.

D. CRITERIA FOR DISSEMINATION.

Information may be disseminated under this section only if it was properly handled under these Procedures. Access to USPI disseminated under this section will be limited to those who need the information to perform an authorized function. USPI may only be disseminated by employees of OIA who have received training on these Procedures and if the information falls in one or more of the following categories:

1. Publicly available. The information is publicly available.

2. Consent. The information concerns only U.S. persons who have consented to the dissemination.

3. Dissemination to another IC element. The dissemination is to another appropriate element of the IC for the purpose of allowing the recipient to determine whether the

information is relevant to its responsibilities and can be retained by it in accordance with its procedures approved by the Attorney General.

4. Dissemination to governmental entities. The dissemination is to an element of Treasury or to any part of a domestic or foreign government and the recipient is reasonably believed to have a need to receive such information for the performance of its lawful functions. For any dissemination under this paragraph that is not consistent with OIA's mission, the Assistant Secretary, or a designee, in consultation with OGC, must approve the dissemination.

5. Assistance to OIA. The dissemination is to a governmental entity, a non-U.S. entity, or an individual or entity not part of a government and is necessary for the limited purpose of assisting OIA to carry out an authorized function. For example, OIA may need assistance in decrypting, translating, or analyzing the information. For such a dissemination, OIA will inform the recipient that (i) it should use the information only for this limited purpose; (ii) it should properly safeguard the information; (iii) it should return or destroy the information when it has provided the requested assistance; and (iv) it should not disseminate the information further without the prior approval of OIA. For any dissemination of USPI to individuals or entities not part of a government under this paragraph, the Assistant Secretary, or a designee, will assess the risk associated with such dissemination (*e.g.,* the risk of misuse or mishandling of the USPI) and whether any further restrictions or handling caveats are needed to protect the information, and shall document that decision in writing.

6. Protective purposes. The dissemination is to a governmental entity, an international entity, or an individual or entity not part of a government, and is necessary to protect the safety or security of persons or property, or to protect against or prevent a crime or threat to the national security. For any dissemination of USPI to individuals or entities not part of a government under this paragraph, the Assistant Secretary or designee, in consultation with OGC, will assess the risk associated with such dissemination (*e.g.,* the risk of misuse or mishandling of the USPI) and whether any further restrictions or handling caveats are needed to protect the information, and shall document that decision in writing.

7. Required dissemination. The dissemination is required by statute; treaty; executive order; Presidential directive; National Security Council directive; policy, memorandum of understanding, or agreement approved by the Attorney General; or court order.

8. Oversight. The dissemination is for oversight purposes. Such dissemination may be to an Executive Branch oversight office, such as the Intelligence Oversight Board or Treasury Office of the Inspector General, or to an appropriate congressional oversight committee in accordance with Treasury policy and guidance.

E. DISSEMINATIONS TO FOREIGN GOVERNMENTS OR ENTITIES.

For any dissemination of USPI to a foreign government or entity, the Assistant Secretary or a designee, in consultation with OGC, must find that the disclosure is consistent with applicable international agreements, information sharing arrangements, and foreign disclosure policy and directives, including those requiring protection against the misuse or unauthorized dissemination of information and the analysis of potential harms to any individual.

F. DISSEMINATIONS OF LARGE AMOUNTS OF UNEVALUATED USPI.

If OIA wishes to disseminate a large amount of USPI under subsections VI.D.4 through VI.D.6 above that has not been evaluated to determine whether it meets the standard for permanent retention, the Assistant Secretary, or a designee, must approve the dissemination in writing, after consulting with OGC and OIA's Civil Liberties and Privacy Protection Officer. The approving official must find that the dissemination complies with the other requirements of this section and that it is not reasonably practicable to accomplish the intended objective by disseminating a lesser amount of USPI. In addition, if the recipient is outside the federal government, the recipient must represent that it has appropriate protections in place, comparable to those required by these Procedures, to safeguard and monitor USPI and to comply with applicable laws; that it will use the information for lawful purposes; and that it will access and retain the information only for those purposes.

G. CONTENT OF DISSEMINATIONS.

OIA should not include USPI in a dissemination if the pertinent information can be understood or its importance assessed without the USPI. If a dissemination includes USPI, OIA will notify the recipient so the recipient can protect the USPI appropriately.

H. IMPROPER DISSEMINATION OF USPI.

OIA will develop policies to address the circumstance when USPI has been disseminated by OIA in error, and when OIA has disseminated information that it originally believed was not USPI but that it later learned was USPI.

I. DISSEMINATION NOT CONFORMING TO THIS SECTION.

Any proposed dissemination that does not conform to the requirements of this section must be approved by OGC, in consultation with the National Security Division of the Department of Justice. Such approval will be made in writing and based on a determination that the proposed dissemination complies with E.O. 12333 and other applicable laws, executive orders, Presidential directives, and ICDs.

VII. PARTICIPATION IN ORGANIZATIONS

A. APPLICABILITY.

This section applies to participation by OIA or anyone acting on behalf of OIA in any organization in the United States, or in any organization outside the United States that constitutes a U.S. person. It does not apply to participation in an organization solely for personal purposes (*i.e.*, activities undertaken on the initiative and at the expense of a person solely for personal benefit). All participation remains subject to applicable Treasury policy. If there is any question about the nature of the participation or whether the person is acting on behalf of OIA, the participant should obtain appropriate guidance.

B. GENERAL DISCLOSURE REQUIREMENT.

OIA employees or anyone else acting on behalf of OIA may join, become a member of, or otherwise participate in an organization in the United States, or in any organization outside the United States that constitutes a U.S. person, if his or her affiliation with OIA is disclosed to an appropriate official of the organization in accordance with subsection F. Without such disclosure, the activity must be permitted by subsections VII.C or VII.D below.

C. EXCLUSIONS.

The requirements of this section do not apply to:

1. Volunteered information. OIA may accept information volunteered by a person who is already a member of an organization, including a person who is participating in an organization solely for personal purposes. If a person provides information in response to a request or tasking by OIA or another element of the IC, OIA may not treat that information as volunteered.

2. Certain activities on the Internet or in other forums. An OIA employee or anyone acting on behalf of OIA may view, research, or collect publicly available information on the Internet or from forums that meet and communicate using technical means, provided that access to the website, service, or forum does not require a true name or affiliation, and there is no elicitation of information or effort to influence the organization or its members.

3. Classes. Attendance by an OIA employee or anyone acting on behalf of OIA at commercial classes or training on non-intelligence skills, when under no direction or tasking to collect intelligence, and the true name and OIA affiliation is used.

4. Publications. Obtaining publications of organizations whose membership is open to the general public.

5. Professional skills. Participation in educational or professional organizations to enhance professional skills, knowledge, or capabilities of employees, when under no direction or tasking to collect intelligence, and the true name and OIA affiliation is used.

D. APPROVAL OF UNDISCLOSED PARTICIPATION.

In accordance with any Treasury policy, and subject to the requirements in subsection VII.E below, an appropriate supervisory OIA official may approve the following kinds of undisclosed participation:

1. Foreign establishments. Participation in an organization that is an official establishment of a foreign government.

2. Seminars and similar events. Attendance at seminars, forums, conferences, exhibitions, trade fairs, workshops, symposiums, and similar meetings, regardless of whether they take place in person or through other means such as social networking sites, sponsored by organizations in which the participant is a member or has been invited to participate, or when the sponsoring organization does not require disclosure of the participants' employment affiliations, to collect significant foreign intelligence that is generally made available to participants at such meetings, and does not involve the domestic activities of the organization or its members.

3. Meetings open to the public. Participation in meetings that are open to the general public. For purposes of this subsection, a seminar or conference sponsored by a professional organization that is open to persons of a particular profession, whether or not they are members of the organization itself or have received a special invitation, will be considered a meeting open to the public.

4. Other undisclosed participation. Undisclosed participation not falling under the categories provided above may be authorized by the Assistant Secretary, or a designee, after consultation with OGC and the National Security Division of the Department of Justice.

E. LIMITATIONS ON UNDISCLOSED PARTICIPATION.

All undisclosed participation must comply with the following requirements:

1. Lawful purpose. The undisclosed participation must be essential to achieving a lawful foreign intelligence or counterintelligence purpose within the assigned mission of OIA, as determined in writing by the Assistant Secretary or a designee. The Assistant Secretary, or a designee, may make a general determination that undisclosed participation in a particular kind of organization or event in identified circumstances is essential to achieving a lawful foreign intelligence or counterintelligence purpose within the assigned mission of OIA.

2. Coordination. The undisclosed participation must be properly coordinated with appropriate agencies in accordance with these Procedures, Sections 1.3(b)(12), 1.3(b)(20), 1.4(h), 1.5(g), and 1.5(h) of E.O. 12333, and any other applicable policies and agreements.

3. Collection methods. Participation by OIA in an organization in the United States, or in an organization outside the United States that constitutes a U.S. person, is limited to overt collection methods or to collecting publicly available information.

4. Compliance with E.O. 12333. All undisclosed participation must comply with the requirements of Section 2.9 of E.O. 12333, including its prohibition of participation undertaken for the purpose of influencing the activities of an organization or its members.

5. Duration of undisclosed participation. Authorization to participate under this section will be limited to the duration of the intelligence activity it is supporting or 12 months, whichever is shorter. An appropriate official must review and re-approve participation for more than 12 months on an annual basis in accordance with this section.

F. MEANS OF DISCLOSURE.

1. General. Unless the undisclosed participation is conducted in accordance with these Procedures, disclosure of the intelligence affiliation of an OIA employee (including anyone else acting on behalf of OIA) must be made to an executive officer of the organization in question, or to an official in charge of membership, attendance, or the records of the organization. Such disclosure must be sufficient to apprise the official of the fact of the person's affiliation with OIA.

2. Employee serving as an official of the organization. If the employee whose participation is at issue is an official of the organization, his or her knowledge alone does not meet the disclosure requirement unless that person is the senior official within the organization. Where the person is not the senior official in the organization, disclosure must be made to an additional official with actual or apparent authority to act on behalf of the organization who is not affiliated with the IC.

3. Who may make disclosure. Disclosure may be made by OIA, by an authorized Treasury official, or by another IC element that is otherwise authorized to take such action on behalf of OIA.

G. RECORDS.

OIA will identify a legal or oversight official to maintain a written record of:

1. The date, time, and manner of any disclosure of intelligence affiliation required by this section, including the name and title of the person to whom the disclosure was made.

2. Any failure to disclose intelligence affiliation required by this section, including the name and title of the person who should have made the disclosure and the circumstances of the failure.

3. Any undisclosed participation conducted by an OIA employee while detailed or assigned to another IC element in accordance with these Procedures.

VIII. SUPPORT TO INTELLIGENCE ACTIVITIES OF OTHER IC ELEMENTS AND SUPPORT TO LAW ENFORCEMENT AGENCIES

A. OTHER IC ELEMENTS.

1. Collection. OIA is authorized, upon request, to support, assist, and cooperate with the foreign intelligence and counterintelligence collection activities of other IC elements. All collection activity must comply with all applicable U.S. laws and be conducted in accordance with these Procedures.

2. Other assistance. OIA may provide, in accordance with OIA policy, technical, analytic, and research assistance to other IC elements. Analytic assistance may include the evaluation of information from other IC elements and the production of "finished" intelligence. Technical assistance means providing other IC elements support or assistance in the form of personnel, equipment, or both where the expertise, knowledge, abilities, capabilities, training, or associations of OIA or contractor personnel will facilitate the U.S. intelligence effort, and includes the provision of devices and training.

   All assistance must comply with all applicable U.S. laws and be conducted in accordance with these Procedures.

3. Detailees and assignees. Unless otherwise provided, when intelligence personnel are detailed to another IC element, the receiving IC element's procedures and authorities will govern. When intelligence personnel are assigned to another IC element, the assigning IC element's procedures and authorities will govern. Individual detail or assignment agreements that depart from these general rules must clearly identify the governing procedures and authorities, be in writing, and be reviewed by legal and other appropriate officials.

B. ASSISTANCE TO LAW ENFORCEMENT AGENCIES.

Consistent with E.O. 12333, applicable laws, other executive orders, Presidential directives, ICDs, and these Procedures, OIA is authorized to cooperate with law enforcement authorities as follows:

1. To protect Treasury and Treasury contractor facilities, property, personnel, and information;

2. Unless otherwise precluded by law or E.O. 12333, to participate in investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities;

3. To provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or, when lives are endangered, to support state or local law enforcement agencies. Provision of the assistance of expert personnel shall be approved in each case by the Assistant Secretary and OGC in writing;

4. To provide assistance to law enforcement agencies and security services of foreign governments or international organizations on a case-by-case basis decided in writing by the Assistant Secretary, in consultation with OGC; and

5. To render any other assistance and cooperation not precluded by applicable law.

Provision of assistance to law enforcement and civil authorities must be approved in each case by OGC in writing.

IX. EMPLOYEE CONDUCT

A. GENERAL.

OIA employees shall conduct intelligence activities only in accordance with E.O. 12333, applicable laws, other executive orders, Presidential directives, ICDs, Treasury policy, and these Procedures.

B. FAMILIARITY WITH RESTRICTIONS.

1. OIA shall familiarize relevant employees with the provisions of E.O. 12333, these Procedures, and any instructions implementing these Procedures that apply to its activities.

2. The Assistant Secretary shall ensure that training is conducted to achieve the requisite familiarity. The training required by this paragraph shall be in person whenever practicable and refreshed at least annually.

C. RESPONSIBILITIES OF THE ASSISTANT SECRETARY.

The Assistant Secretary will:

1. Ensure that no adverse action is taken against any employee for reporting activities pursuant to Section X.

2. Impose such sanctions as may be appropriate under Treasury regulations, orders, and policies upon any employee who violates the provisions of these Procedures or any instructions, policies, or guidance promulgated thereunder.

3. In any case involving a breach of security regulations and guidelines by either Treasury or non-Treasury employees, notify the appropriate investigative agency within Treasury.

4. Ensure that, to the extent consistent with applicable law and privileges, legal, oversight, privacy, and civil liberties officials and the Inspector General have access to appropriate information concerning the intelligence activities of OIA necessary to perform their oversight responsibilities.

5. Ensure that, to the extent consistent with applicable law and privileges, OIA employees cooperate fully with the Intelligence Oversight Board (IOB) and its representatives.

X. COMPLIANCE, OVERSIGHT, AND REPORTING

A. GENERAL PROTECTIONS FOR USPI.

1. Responsibilities of OIA. For all USPI, OIA will:

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

   b. When retrieving information electronically:

      i. Only use queries or other techniques that are intended to retrieve information relevant to the intelligence mission or other authorized purposes.

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

iii. Establish written procedures to document the basis for conducting queries of unevaluated information that are intended to reveal USPI.

c. Take reasonable steps to audit access to information systems containing USPI and to audit queries or other search terms to assess compliance with these Procedures.

d. In developing and deploying new information systems containing USPI, take reasonable steps to ensure effective auditing and reporting as required by these Procedures.

e. Establish documented procedures for retaining data containing USPI, recording the reason for retaining the data, and identifying which officials have authority to approve the retention.

f. Regularly train employees who access or use USPI on the civil liberties and privacy protections that apply to such information.

g. Adhere to such other requirements as may be established by OIA.

2. Marking electronic and paper files. OIA will use reasonable measures to design and develop information systems to identify and mark or tag files (including emails, attachments, automated systems, and all paper files) that are reasonably believed or known to contain USPI. Marking and tagging will occur regardless of the format or location of the information, or the method of storing it. When appropriate and reasonably possible, OIA will also mark files and documents containing USPI individually. In the case of certain electronic databases, if it is not reasonably possible to mark individual files containing USPI, OIA may use a banner informing users prior to access that they may encounter USPI.

3. Reviews. Oversight personnel designated by the Assistant Secretary, or a designee, will periodically review OIA's practices for protecting USPI in accordance with these Procedures.

B. COMPLIANCE AND OVERSIGHT.

E.O. 13462, as amended, established the IOB in order to enhance the security of the United States by assuring the legality of the activities of the IC. The Assistant Secretary, in consultation with OGC, will report intelligence activities they have reason to believe are unlawful, or contrary to Presidential order or directive, to the IOB to the extent required by Section 1.6(c) of E.O. 12333; E.O. 13462; and criteria issued by the IOB.[4] To the extent permitted by law and consistent with any applicable privileges, the Assistant Secretary will also provide the IOB with all information necessary to carry out

[4] Available through the DNI's publicly available website.

its responsibilities. The Assistant Secretary will provide a copy of all reports to the DNI. This section addresses OIA's compliance and oversight responsibilities, and the requirements for reporting of questionable intelligence activities. To the extent consistent with applicable law and privileges, all OIA employees and contractors will cooperate fully with the IOB.

1. OIA policies and guidance issued to implement these Procedures shall include appropriate measures to facilitate compliance and oversight. OIA information systems will, to the extent possible, facilitate auditing of access to and queries of information relevant to OIA's intelligence activities.

2. The Assistant Secretary or designee shall establish guidance for the implementation of these Procedures and for other issues as required, establish oversight mechanisms (such as periodic audit and review).

3. The Assistant Secretary shall appoint a Civil Liberties and Privacy Protection Officer who shall be responsible for providing advice and assistance to the Assistant Secretary and other senior Treasury officials regarding privacy and civil liberties concerns in implementing these Procedures, and for implementing the oversight and compliance functions in these Procedures.

4. As part of its independent responsibilities, the Office of the Inspector General shall conduct audits, inspections, and investigations of OIA programs to determine compliance with applicable statutes and regulations, including these Procedures.

5. OGC 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 and other U.S. Government entities regarding these Procedures.

6. The heads of OIA offices shall implement these Procedures in coordination with the Assistant Secretary, or a designee, and provide training to employees who require access in the performance of their duties to information governed by these Procedures.

7. OIA employees are responsible for becoming familiar with and complying with these Procedures and any implementing guidance, referring any questions concerning the interpretation of these Procedures to OGC, using the information that is subject to these Procedures for only lawful and authorized purposes, and reporting activities that may be unlawful or contrary to executive order or Presidential directive to the appropriate chain of command, OGC, or Treasury's Office of the Inspector General.

C. QUESTIONABLE INTELLIGENCE ACTIVITIES.

1. Definition. A questionable intelligence activity is an intelligence activity that may violate the law, E.O. 12333, any other executive order or Presidential directive, or applicable Treasury policy, including these Procedures.

2. Identification. Each OIA employee must report any questionable intelligence activity to the Assistant Secretary, or a designee, and to an appropriate oversight official.

3. Investigation.

   a. Each report of questionable intelligence activity will be investigated to the extent necessary to determine the facts and assess whether the activity is legal and consistent with applicable policy.

   b. Investigations will be conducted expeditiously. The officials responsible for these investigations may, in accordance with established procedures, obtain assistance from OIA, or from other Treasury components, as necessary to complete the investigations in a timely manner.

   c. Investigations will be conducted in accordance with Presidential Policy Directive 19, Protecting Whistleblowers with Access to Classified Information, and other applicable law and Treasury policy.

D. REPORTING TO THE ATTORNEY GENERAL.

All reports made under subsections X.B or X.C above that involve a possible violation of federal criminal law will be sent to the Attorney General after consultation with OGC, in accordance with the procedures adopted under Section 1.6(b) of E.O. 12333.

XI. GENERAL PROVISIONS

A. ACTIVITIES CONDUCTED FOR ADMINISTRATIVE PURPOSES.

OIA may collect USPI for administrative purposes. Information is collected for administrative purposes when it is necessary for the administration of OIA but is not collected directly for intelligence purposes. Information collected for administrative purposes includes: information about systems administration, contracting, public affairs and legislative matters, personnel training, security records and files, and training materials. Nothing in these Procedures prohibits the collection, retention, or dissemination of such information by OIA or another component authorized to engage in such functions.

B. DELEGATION.

When these Procedures require a specific Treasury official to approve an activity or take some other action, only that official, or a more senior official, may take that action. When these Procedures permit an official to delegate responsibility for an action, the official may delegate the responsibility to one or more appropriate officials in accordance with Treasury policy, unless specifically limited to a single designee.

C. INTERPRETATION.

The Assistant Secretary, together with OGC, will consult with the Assistant Attorney General for National Security and the Office of the Director of National Intelligence (ODNI) regarding any novel or significant interpretations of these Procedures.

D. DEPARTURES.

The Assistant Secretary and the Assistant Attorney General for National Security, after consultation with OGC and ODNI, must approve in advance any departures from these Procedures. If there is not time for such approval and a departure from these Procedures is necessary because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, the Assistant Secretary may approve a departure from these Procedures. OGC will be notified as soon as possible. The Assistant Secretary will provide prompt written notice of any such departures to the Assistant Attorney General for National Security and ODNI. All activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

E. AMENDMENTS.

Substantive amendments to these Procedures require the approval of the Secretary and the Attorney General, after consultation with the DNI.

F. TRANSITION.

OIA will implement these Procedures in accordance with guidance from the Assistant Secretary and will have 18 months from the effective date of these Procedures to implement the requirements of these Procedures.

G. EFFECT.

These Procedures are set forth solely for the purpose of internal Treasury guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person, nor do they place any limitation on otherwise lawful investigative and litigative prerogatives of the United States.

XII. DEFINITIONS

The following definitions apply to these Procedures:

Collection. Information is "collected" when it is received by OIA, whether or not it is retained by OIA for intelligence or other purposes. Collected information includes information obtained or acquired by any means, including information that is volunteered to OIA. Collected information does not include (i) information that only momentarily passes through an OIA computer system; (ii) information on the Internet or in an electronic forum or repository outside OIA that is simply viewed or accessed by an OIA employee but is not copied, saved, supplemented, or used in some manner; (iii) information disseminated to OIA by other IC elements; or (iv) information that is maintained on behalf of another U.S. Government agency and to which OIA does not have access for intelligence purposes.

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 where legally adequate notice has been provided. Consent may also be implied where a legally adequate policy has been published or otherwise circulated. OGC will determine whether a notice or policy is adequate and lawful before OIA relies on implied consent to take or refrain from taking an action on the basis of the consent.

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.

Dissemination means the transmission, communication, sharing, or passing of information outside OIA by any means, including oral, electronic, or physical means. It therefore includes providing any access to information in OIA's custody to a person outside OIA.

Domestic activities means activities that take place in the United States and do not involve a significant connection with either an agent of a foreign power or a foreign power, organization, or person.

Electronic surveillance means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

Employee, when referring to any Treasury employee, means any person employed by Treasury; any person employed by another agency and working under the direction and

control of Treasury; or an employee of a Treasury contractor or subcontractor. A source is not an employee.

Foreign economic information means information relating to foreign economic resources, activities, and policies, including the production and consumption of goods and services, labor, finance, taxation, trade, other aspects of foreign economies, and the foreign aspects of the international economic system.

Foreign financial information means information relating to the monetary support and resources of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

Foreign intelligence means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists. Foreign intelligence includes foreign financial information and foreign economic information.

Foreign power means:

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

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

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

d. A group engaged in international terrorism or activities in preparation therefor;

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

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

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

Host of a shared repository means an entity responsible for developing and maintaining a shared repository. A host may or may not have access to information in the repository for intelligence or other operational purposes. A host may be a governmental or private-sector entity.

Incidental collection of USPI means collection of USPI that is not deliberately sought by OIA, but that is nonetheless collected. Collection of USPI that is not deliberately sought is considered incidental regardless of whether it is expected or reasonably anticipated to occur.

Intelligence includes foreign intelligence (including foreign financial intelligence and foreign economic intelligence) and counterintelligence.

Intelligence activities means all activities that elements of the IC are authorized to conduct under E.O. 12333.

Intelligence Community (IC), elements of the IC, and IC elements mean those agencies and elements described in Section 3.5(h) of E.O. 12333.

Intentional collection of USPI means collection of USPI that is deliberately sought by OIA.

International terrorism and international terrorist activities means activities that (1) involve violent acts or acts dangerous to human life that violate domestic criminal law or would violate such law if committed in the United States or a state, local, or tribal jurisdiction; (2) appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by assassination or kidnapping; and (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

Join means to become a member of, or become associated with, an organization, with or without the payment of dues or membership fees.

Organization, for purposes of section VII and for purposes of the definitions of "organization in the United States," "participation," "participation on behalf of OIA," "participation undertaken for the purpose of influencing the activities of an organization," and "undisclosed participation," means an association of two or more individuals formed for any lawful purpose whose existence is formalized in some manner. The term includes social, political, fraternal, professional, business, academic, ethnic-affinity, and religious organizations. The term includes organizations that meet and communicate primarily on the Internet or through the use of other technologies. It does not include a loose group of friends, social contacts, or business associates who may share common interests but whose association lacks any formal structure. For example, the Rotary Club is an organization; a group of friends who play poker or meet at a gym for athletics every weekend is not.

Organization in the United States means an organization physically located in the United States, whether or not it constitutes a U.S. person. Thus, a branch, subsidiary, or office of

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

Overt collection means either (i) collection that is openly acknowledged by or is readily attributable to the U.S. Government, or (ii) collection where no steps are taken to conceal the U.S. Government collection activity and the role of the U.S. Government would be acknowledged in response to an express inquiry. Acknowledgment may include advising of U.S. Government affiliation (confirming the collector's affiliation with an intelligence element is not required, so long as U.S. Government affiliation is acknowledged) or advising of a general collection activity applicable to that individual (rather than advising of specific acquisition methods, sites, or processes being used, or other details about the collection).

For example, in accordance with its established procedures, OIA might monitor Government-furnished equipment based on notice to the individuals from whom the information is collected, but OIA would not need to provide the details of the monitoring, or acknowledge which specific users it had chosen to monitor.

Participation means taking part in an organization's activities and interacting with its members within the structure or framework of the organization. Such actions include, but are not limited to, joining or acquiring membership; attending or taking part in organizational meetings, academic activities, seminars, trade fairs, workshops, conferences, exhibitions, symposiums, social functions, or forums for Internet or other communications; carrying out the work or functions of the organization; serving as a representative or agent of the organization; and contributing funds to the organization other than in payment for goods or services. Participation does not include occasional passive attendance at forums that are open to the public, including non-members. In addition, participation does not include taking part in events outside the organizational structure or framework, such as infrequent attendance at meetings or occasional social gatherings that involve the organization's members, but that are not functions or activities conducted on behalf of the organization itself.

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

Participation undertaken for the purpose of influencing the activities of an organization means any action taken with the intention of causing a significant effect on the

organization's agenda, course of business, core activities, or future direction. Simply voting or expressing an opinion on these matters as a member will generally not fall within this definition.

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

Retention means the maintenance of information in either hard copy or electronic format regardless of how the information was collected or how it was disseminated to OIA by another element of the IC.

Shared repository means a database, environment, or other repository maintained for the use of more than one entity. A database, environment, or other repository that a contractor or other entity maintains for the use of only OIA, or those acting on its behalf, is not a shared repository.

Undisclosed participation means participation by an OIA employee or other person acting on behalf of OIA in any organization in the United States, or any organization outside the United States that is a U.S. person, if the person's intelligence affiliation with OIA is not disclosed to an appropriate official of the organization.

U.S. person means any of the following:

a. A U.S. citizen, including persons with dual U.S./foreign citizenship;

b. An alien known by OIA to be a permanent resident alien;

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

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

In applying paragraph c, if a group or organization in the United States that is affiliated with a foreign-based international organization operates directly under the control of the international organization and has no independent programs or activities in the United States, the membership of the entire international organization will be considered in determining whether it is substantially composed of U.S. persons. If, however, the U.S.-

based group or organization has programs or activities separate from, or in addition to, those directed by the international organization, only its membership in the United States will be considered in determining whether it is substantially composed of U.S. persons. Unless specific information to the contrary is obtained, a person or organization in the United States is presumed to be a U.S. person and a person or organization outside the United States, or whose location is not known to be in the United States, is presumed to be a non-U.S. person.

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

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

USPI does not include a reference to a product by brand or manufacturer's name or the use of a name in a descriptive sense, as, for example, "Ford Mustang" or "Boeing 787." Imagery from overhead reconnaissance or information about conveyances, such as vehicles, aircraft, or vessels, should not be considered USPI without linkage to additional identifying information that ties the information to a specific U.S. person.

---- Remainder of this page intentionally left blank. ----

We approve the foregoing Procedures in accordance with E.O. 12333, as amended.

Janet L. Yellen
Secretary of the Treasury

DEC 0 6 2022
Date

Merrick B. Garland
Attorney General

6/14/23
Date