January 17, 2017

DEPARTMENT OF ENERGY PROCEDURES FOR INTELLIGENCE ACTIVITIES

PROCEDURES FOR INTELLIGENCE ACTIVITIES
TABLE OF CONTENTS

INTRODUCTION — Page

I. APPLICABILITY AND SCOPE
- A. Intelligence activities 1
- B. DOE Intelligence Components 1
- C. Management and operating contractors 1

II. AUTHORIZED ACTIVITIES AND COORDINATION
- A. General 1
- B. Conduct of activities and indirect participation 2
- C. Research, analysis, and assessments 2
- D. Counterintelligence inquiries and investigations 2
- E. Shared repositories 3
- F. Coordination 4

III. COLLECTION OF USPI
- A. Intentional collection of USPI 5
- B. Incidentally collected or voluntarily provided USPI 7
- C. Collection involving special circumstances 7
- D. Least intrusive means 8
- E. Amount of information collected 8

IV. COLLECTION TECHNIQUES
- A. General 8
- B. Use of techniques 8
- C. Equipment monitoring 9
- D. Physical surveillance 10
- E. Consensual physical searches 11
- F. Other techniques 11

V. RETENTION OF USPI
- A. Applicability 12
- B. Evaluation of information 12
- C. Information disseminated by another Component or IC element 13
- D. Permanent retention 13
- E. General protections for USPI 14
- F. Enhanced safeguards 15
- G. Retention for backup purposes 16

VI. DISSEMINATION OF USPI
- A. Applicability and scope 16
- B. Consistency with other laws 16
- C. Criteria for dissemination 16

D. Disseminations to foreign governments or entities 17
E. Disseminations of large amounts of unevaluated USPI 17
F. Content of disseminations 18
G. Improper dissemination of USPI 18
H. Disseminations not conforming to this section 18

VII. PARTICIPATION IN ORGANIZATIONS
A. Applicability 18
B. General disclosure requirement 18
C. Activities for which no specific approval or disclosure is required 18
D. Meetings open to the public 19
E. Other undisclosed participation requiring approval 19
F. Limitations on undisclosed participation 19
G. Means of disclosure 20
H. Records 20

VIII. SUPPORT TO INTELLIGENCE ACTIVITIES OF OTHER IC ELEMENTS AND SUPPORT TO LAW ENFORCEMENT AGENCIES
A. Intelligence collection activities of other IC elements 21
B. Provision of expert capabilities to other IC elements 22
C. Assistance to law enforcement agencies 22

IX. CONTRACTING FOR GOODS AND SERVICES
A. General 23
B. Procedures 23

X. EMPLOYEE CONDUCT
A. General 24
B. Familiarity with restrictions 24
C. Responsibilities of heads of DOE Intelligence Components 24

XI. OVERSIGHT REPORTING
A. General 24
B. Questionable intelligence activities 25
C. Reporting to the Attorney General 25

XII. GENERAL PROVISIONS
A. Activities conducted for administrative purposes 25
B. Delegation 26
C. Interpretation 26
D. Departures 26
E. Transition 26
F. Effect 26

XIII. DEFINITIONS 26

INTRODUCTION

These Department of Energy (DOE) Procedures for Intelligence Activities ("Procedures") are intended to enable DOE Intelligence Components to carry out their authorized functions effectively; to provide appropriate assistance to other elements of the Intelligence Community (IC); and to ensure that DOE intelligence activities and programs are carried out in a manner consistent with the constitutional rights of US persons and other protections provided under applicable law and policy. These Procedures govern how DOE Intelligence Components 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 any DOE component, in the United States or abroad. These Procedures do not apply to non-intelligence activities conducted by DOE intelligence components.

B. DOE INTELLIGENCE COMPONENTS. DOE Intelligence Components are:

1. The Secretary of Energy, when acting in an intelligence capacity, and

2. The Office of Intelligence and Counterintelligence (IN) and subordinate offices. The Director of IN ("Director") designates subordinate offices that include, but are not limited to, IN headquarters directorates, Field Intelligence Elements, and counterintelligence field offices.

C. MANAGEMENT AND OPERATING CONTRACTORS. These Procedures apply to all DOE management and operating contractors and their subcontractors and employees engaged in intelligence activities, including, but not limited to:

1. Work sponsored by an organization identified in EO12333 as an element of the IC;

2. Work funded by either the National Intelligence Program or the Military Intelligence Program; and

3. Work for which the DOE Headquarters official is the Director.

II. AUTHORIZED ACTIVITIES AND COORDINATION

A. GENERAL. In accordance with EO 12333 and these Procedures, DOE Intelligence Components may collect information in support of national and departmental missions as set forth in the Atomic Energy Act, the DOE Organization Act, the Nuclear Nonproliferation Act, EO 12333, and other applicable executive orders, Presidential directives, and Intelligence Community Directives (ICDs). These activities are authorized as part of research, analysis and assessments under subsection C or as part of counterintelligence inquiries and investigations under subsection D. Activities conducted in support of collection activities of other IC elements and law enforcement agencies are governed by section VIII. DOE Intelligence Components must coordinate all activities in accordance with subsection F.

B. CONDUCT OF ACTIVITIES AND INDIRECT PARTICIPATION. DOE Intelligence Components must carry out all activities in all circumstances in accordance with the Constitution and laws of the United States. Components may not investigate US persons, or collect or maintain information about them, solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States. Further, Components may not participate in or request any person or entity to undertake any activities that are forbidden by EO 12333 or these Procedures. In accordance with the authorities and responsibilities described in these Procedures, DOE Intelligence Components are 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 by DOE 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 General Counsel of DOE.

C. RESEARCH, ANALYSIS, AND ASSESSMENTS. A DOE Intelligence Component may conduct research, analysis and assessments to detect, obtain information about, or prevent or protect against international terrorism, the 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 and to collect foreign intelligence, in accordance with DOE policy and EO 12333. A Component may conduct research, analysis and assessments proactively to collect new information or draw on available information previously collected pursuant to these Procedures. A Component conducting research, analysis, and assessments may only collect US person information (USPI) in accordance with section III, and may use only the techniques identified in subsections IV.B.1 and F.

D. COUNTERINTELLIGENCE INQUIRIES AND INVESTIGATIONS

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

2. USPI. As part of a counterintelligence inquiry or investigation, a DOE Intelligence Component may collect USPI provided that it does so in accordance with section III and that any US person about whom the Component is intentionally seeking information falls in one or more of the following categories:

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

      Example: A scientist in a foreign country who is both a citizen of that country and a US permanent resident alien and who is or will be coming for six months to work at a DOE laboratory.

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

c. Employees traveling to foreign countries. A DOE employee in contact with a non-US person or dual national outside the US.

Example: An employee of a DOE contractor who voluntarily reports an unusual contact with a purported scientist from a foreign country while at a conference outside the US.

d. Hostile activities. A DOE or DOE contractor employee or former employee reasonably believed to be engaged in international terrorism; unauthorized intelligence collection targeting the United States; or other hostile activities.

e. Other US persons. Any other US person in contact with a DOE or DOE contractor employee or former employee when such other person is reasonably believed to be engaged in international terrorism; unauthorized intelligence collection targeting the United States; or other hostile activities.

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

E. SHARED REPOSITORIES. A DOE Intelligence Component may host or participate in a shared repository containing USPI only in accordance with these Procedures and other applicable laws and policies.

1. Component acting as host. A Component 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. A host Component must enable audit of access to USPI in a shared repository to the extent practicable. Each participant in a shared repository must inform the host Component in writing that its participation complies with all law, policies, and procedures applicable to the protection of USPI.

2. Component acting as participant. A Component acting as a participant in a shared repository must ensure that its access to and use of the repository complies with law, policies, and procedures applicable to the protection of USPI (including these Procedures), and must identify to the host any access and use limitations applicable to the USPI it provides. A participating Component that provides USPI to a shared repository and allows access to or use of the USPI by other participants has made a dissemination, and may do so only in accordance with section VI 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.

F. COORDINATION. DOE Intelligence Components will coordinate activities as follows:

1. Counterintelligence activities in the United States. A DOE Intelligence Component 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 FBI. In addition:

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

    b. Any indication that classified information may have been disclosed in an unauthorized manner 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 of Energy or a designee will promptly inform the Attorney General and the Director of National Intelligence (DNI) if DOE engages in counterintelligence activities in the United States that have not been coordinated with the FBI. The Secretary or 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 EO 12333 authorizes DOE Intelligence Components to collect information overtly or through publicly available means. Unless acting under the authority of another IC element as provided in section VIII, Components are not authorized to collect information clandestinely. The Secretary of Energy or a designee will promptly inform the Attorney General and the DNI if DOE engages in the clandestine collection of foreign intelligence in the United States, other than as specifically authorized in section VIII. The Secretary or designee will inform the Attorney General through the FBI, and will also notify the Assistant Attorney General for National Security.

3. Activities outside the United States. A DOE Intelligence Component must coordinate counterintelligence activities outside the United States with the CIA. The Secretary of Energy or a designee will promptly inform the Director of the CIA and the DNI if DOE engages in such activities outside the United States that have not been coordinated with the CIA. The Secretary or a designee will similarly inform the Director of the CIA and the DNI if DOE engages in the clandestine collection of foreign intelligence outside the United States, unless the collection is under the authority of another IC element and is specifically authorized under section VIII.

4. Compliance with agreements. DOE Intelligence Components will comply with all agreements and memoranda of understanding with the Department of Justice, the FBI,

and the CIA governing the coordination of activities covered by this section, as applicable to each DOE Intelligence Component.

III. COLLECTION OF USPI

A. INTENTIONAL COLLECTION OF USPI. A DOE Intelligence Component may intentionally collect USPI only (i) in accordance with sections II and IV, (ii) if the information sought is reasonably believed to be necessary for the performance of an authorized mission or function assigned to the Component, and (iii) if the information falls in one or more of the following categories:

1. Publicly available. The information is publicly available. An example is information posted on the Internet with no access controls.

2. Consent. The information concerns a US person who has consented to the collection. An example is information provided by individuals who consent to computer monitoring in accordance with section IV.C.

3. Foreign intelligence. The information is reasonably believed to be foreign intelligence and the US person is one of the following:

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

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

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

   d. An individual, organization, or group reasonably believed to be engaged in or preparing for, on behalf of a foreign power, attacks on or intrusions into DOE information systems; DOE contractors' information systems that impact DOE personnel, property, or missions; or US Government national security systems.

   e. An individual, organization, or group reasonably believed to be engaged in or preparing to target, exploit, or illegally divert DOE or related technology on behalf of a foreign power.

   f. 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.

   g. 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.

   h. Corporations or other commercial entities or organizations, or individuals employed by or working on behalf of such companies or organizations, reasonably believed to be conducting or preparing to conduct business with a foreign power, organization, or person, and such business would impact foreign energy matters or the weapons of

mass destruction or disruptive science and technology capabilities of a foreign power, a foreign organization, or an international terrorist organization.

4. Counterintelligence. The information is reasonably believed to be counterintelligence and the information is acquired as part of properly authorized and conducted research, analysis and assessments under section II.C or a counterintelligence inquiry or investigation under section II.D.

5. Current, former, or potential sources of assistance to intelligence activities. USPI may be collected 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 DOE employees. This category does not include investigations undertaken for personnel security purposes.

6. Protection of intelligence sources, methods, and activities. USPI may be collected 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 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 US persons who fall in one of the following categories:

   a. Present or former DOE Intelligence Component employees.

   b. Present or former DOE Intelligence Component contractors.

   c. Present or former employees of present or former DOE Intelligence Component contractors.

   d. Applicants seeking employment with a DOE Intelligence Component or a DOE Intelligence Component contractor.

   Otherwise, a DOE Intelligence Component may not collect such information in the United States unless done as support to other agencies under section VIII.

7. Threats to safety. USPI may be collected about a person when the information is needed to protect the safety of DOE and energy-critical infrastructure, facilities, personnel, programs, contractors, or official visitors, including those who are targets, victims, or hostages of international terrorist activities.

8. Physical security. USPI may be collected about a person reasonably believed to threaten the physical security of DOE facilities, personnel, programs, contractors or official visitors. USPI may also be collected arising out of a lawful physical security investigation.

9. Personnel security investigations. USPI may be collected about a person arising out of a lawful personnel security investigation. Such USPI may include information contained in personnel files.

10. Communications security. USPI may be collected about a person arising out of a lawful communications security investigation.

11. Network security. USPI needed for network security, cyber security, and incident response may be collected if the information otherwise falls into one of the categories in paragraphs 1 through 10 above. Equipment monitoring must also comply with the requirements of subsection IV.C.

12. Insider threats. USPI needed for insider threat detection or prevention purposes may be collected if the information otherwise falls into one of the categories in paragraphs 1 through 10 above.

13. Supply chain protection. USPI needed for energy and technology supply chain risk management efforts may be collected if the information otherwise falls into one of the categories in paragraphs 1 through 10 above.

14. Special Nuclear Material, Restricted Data, or other classified and unclassified sensitive information. USPI may be collected that is necessary to protect Special Nuclear Material, Restricted Data, Formerly Restricted Data, National Security Information and Unclassified Controlled Nuclear Information, as defined in the Atomic Energy Act of 1954.

15. Overhead reconnaissance. USPI acquired by overhead reconnaissance not directed at specific US persons may be collected.

B. INCIDENTALLY COLLECTED OR VOLUNTARILY PROVIDED USPI. In the course of authorized activities, a DOE Intelligence Component may incidentally collect USPI. Entities or individuals may also on their own initiative voluntarily provide information to a Component. All incidentally collected or voluntarily provided information is "collected" for purposes of these Procedures and may be temporarily retained, evaluated for permanent retention, and disseminated only in accordance with sections V and VI. If an entity or individual is voluntarily providing on a recurring basis USPI that is not relevant to an authorized mission or function assigned to the Component, the Component should either request that the entity or individual stop providing the USPI or take other appropriate steps, such as promptly purging or returning the information.

C. COLLECTION INVOLVING SPECIAL CIRCUMSTANCES. Pursuant to guidance issued by the Director after consultation with privacy and civil liberties officials, a DOE Intelligence Component will consider whether collection opportunities require higher-level approval and consideration of enhanced safeguards because of the volume, proportion, or sensitivity of the USPI likely to be acquired. When such special circumstances exist, the Head of the Component or a delegee must determine, after consulting with the National Security Division of the Department of Justice and the Office of the Director of National Intelligence (ODNI), whether to authorize the collection. If advance authorization is not possible, then as soon as possible after collection the Component head or delegee must authorize the continued retention of the information in accordance with paragraphs 1 and 2 below and section V.B. The determination will be based on the following:

1. Proper collection. The information has been or will be properly collected in accordance with paragraph A and the other provisions of this section; and

2. Reasonable under the circumstances. The collection activity is reasonable based on all the circumstances, including the value of the information; its impact, duration, and resources utilized; the collection methods used by the Component or others; the amount of USPI; the nature and sensitivity of the USPI; the potential for substantial harm, embarrassment, inconvenience, or unfairness to US persons if the USPI is improperly used or disclosed; and the safeguards that will be applied to the information under section V.

The DOE Intelligence Component will provide a copy of all such determinations to appropriate privacy and civil liberties officials. In addressing questions about the implementation of this provision, a Component will consult with its privacy and civil liberties officials.

D. LEAST INTRUSIVE MEANS. DOE intelligence Components will use the least intrusive, but still effective, collection techniques feasible within the United States or against a US person abroad. This requirement is not intended to discourage Components from seeking needed intelligence. They should, however, consider the privacy interests of any US person, and any potential harm to such person's reputation. Generally, collection from publicly available sources or collection with the consent of the person concerned is less intrusive than other techniques.

E. AMOUNT OF INFORMATION COLLECTED. Subject to paragraph D above, in collecting non-publicly available USPI, a DOE Intelligence Component will, to the extent practicable, collect no more information than is reasonably necessary.

IV. COLLECTION TECHNIQUES

A. GENERAL. DOE Intelligence Components may use the techniques authorized in this section to collect information. All activities must conform to the requirements of section II, including its coordination requirements, and all collection of USPI must conform to the requirements of section III. In accordance with section 1.7(i) of EO 12333, DOE Intelligence Components may only collect information overtly or through publicly available means. This limitation applies to any technique used, whether inside or outside the United States. Components do 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 a Component believes that there is a need to use such a technique, it should consult with legal counsel and consider whether another IC element with the appropriate authority can engage in the activity.

B. USE OF TECHNIQUES

1. Research, analysis and assessments. As part of authorized research, analysis and assessments, a DOE Intelligence Component may use the following techniques:

   a. Obtain publicly available information.

   b. Access and examine DOE records and obtain information from DOE personnel.

c. Access and examine records maintained by, and request information from, other federal, state, local, tribal, or foreign governmental entities or agencies.

d. Use online services and resources (whether nonprofit or commercial).

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 or investigation.

f. Conduct equipment monitoring in accordance with subsection C.

2. Counterintelligence inquiries. As part of an authorized counterintelligence inquiry, a DOE Intelligence Component may use the following techniques:

a. All techniques authorized for research, analysis and assessments.

b. Witness interviews.

c. Subject interviews.

d. Assistance to law enforcement and other civil authorities in accordance with subsection VIII.C.

3. Counterintelligence investigations. As part of an authorized counterintelligence investigation, a DOE Intelligence Component may use the following techniques:

a. All techniques authorized for research, analysis and assessments and counterintelligence inquiries.

b. Physical surveillance in accordance with subsection D.

c. Consensual physical searches in accordance with subsection E.

d. Intelligence collection in support of an IC element in accordance with subsection VIII.A.

C. EQUIPMENT MONITORING

1. General. A DOE Intelligence Component may monitor equipment belonging to DOE and others, including computer systems, mobile devices, and telephones, or obtain the results of such monitoring, in accordance with paragraphs 2 through 4 below. The Director will promulgate a policy to govern monitoring, and the Component will conduct all monitoring in accordance with the policy and the requirements of this subsection.

2. DOE equipment. Before monitoring DOE equipment, a DOE Intelligence Component will obtain users' consent and properly notify users that their communications and activities will be monitored. The DOE entity responsible for or operating the monitored equipment will implement this requirement by use of some or all of the following means in a way that is sufficient to obtain consent and provide proper notice:

a. Periodic acknowledgements by users.

b. Decals placed on devices being monitored.
c. User agreements acknowledging that monitoring may occur, and the use that the Government may make of any information on or obtained from the equipment.
d. Specific memoranda to users.
e. Standing operating procedures and instructions.
f. Workplace training that specifically addresses terms of monitoring.

Whenever reasonably feasible, a DOE Intelligence Component or the DOE entity responsible for or operating the monitored equipment will require periodic acknowledgement by users that their use of such systems constitutes consent to monitoring and require such other acknowledgements or consent as may be appropriate. Such acknowledgements may be in electronic form.

3. Contractor equipment. A DOE Intelligence Component may monitor equipment belonging to a Government contractor, or serving the contractor's spaces or requirements, if it has an express authorization in a contract with the contractor or if it obtains periodic express written approval of the chief executive officer, or a designee, of the contractor organization. In either case, the Intelligence Component's advising legal office must periodically make a written finding that sufficient measures, such as those described in paragraph 2 above, have been implemented to obtain the consent of the contractor organization's employees. In making this finding, the advising legal office may rely on reasonable factual representations made by the contractor organization as to the content of banners on the monitored equipment, the details of user agreements, and similar matters relating to how the contractor organization provides notice to and obtains consent from its employees.

4. Other equipment. A DOE Intelligence Component may monitor other equipment, not covered by paragraph 2 or 3 above, or obtain the results of such monitoring, when such equipment is present on DOE sites, locations, or facilities or is connected to DOE systems. Any such monitoring requires the consent of the individuals or entities subject to the monitoring and must comply with relevant statutory and constitutional provisions. Before the start of the monitoring and periodically thereafter, the Component's advising legal office must make a written finding that sufficient measures, including those required by paragraph 2 above, establish that the individuals or entities subject to the monitoring have consented to it. In making this finding, the advising legal office 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 is monitored.

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

D. PHYSICAL SURVEILLANCE. A DOE Intelligence Component may conduct physical surveillance of the subject of a counterintelligence investigation, provided that the investigation is approved as provided in section II.D.3 and that:

1. The subject of the investigation is:

a. A non-US person; or

b. A US person who is a present or former employee of a DOE Intelligence Component, a present or former contractor of an intelligence component or their present or former employees, or an applicant for such employment or contracting.

2. The physical surveillance is being conducted on DOE sites, facilities, or property.

3. The information that will be acquired from the physical surveillance must be publicly available or, if any part of the information will not be publicly available, the surveillance to acquire that information must be conducted overtly;

4. The Component has coordinated the surveillance in accordance with subsection II.F; and

5. The Director or a single designee has approved the surveillance in writing after consulting with advising legal counsel. The approving official may authorize the surveillance initially, or renew it periodically, for periods up to 90 days.

E. CONSENSUAL PHYSICAL SEARCHES. A DOE Intelligence Component 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 DOE or contractor facility and (ii) is used by a subject of a counterintelligence investigation, provided that an investigation is open as provided in section II and provided that:

1. The subject of the investigation is:

a. A non-US person; or

b. A US person who is a present or former employee of DOE, a present or former contractor of DOE, a present or former employee of a DOE contractor, or an applicant for such employment or contracting.

2. The subject of the investigation (or any other person whose office space, furniture, or personal items is being searched) has consented to the search, and advising legal counsel 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 investigation(s).

3. The Component has coordinated the search in accordance with section II.F.

F. OTHER TECHNIQUES. A DOE Intelligence Component may use any technique not specifically covered in this section with the approval of the Director after consultation with legal counsel, provided that use of the technique is consistent with the limitations of subsection A and EO 12333. A Component may conduct polygraph examinations in accordance with 10 C.F.R. § 709, or any successor regulation or other applicable regulation or law.

V. RETENTION OF USPI

A. APPLICABILITY. This section governs DOE Intelligence Components' retention of USPI 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 DOE Intelligence Component or element of the IC is governed by paragraphs C through G.

B. EVALUATION OF INFORMATION. A DOE Intelligence Component will evaluate information that may contain USPI to determine whether it may be permanently retained under paragraph D below, as follows:

1. Intentional collection of USPI. If a Component intentionally collects USPI, the Component will evaluate the information promptly. If necessary, the Component may retain the information for evaluation for up to five years. The Director may approve an extended period in accordance with paragraph B.5 below.

2. Incidental collection of USPI. A Component may intentionally collect information about a target that, at the time of collection, is inside or outside the United States. If a Component does so and incidentally may have collected USPI, the Component may retain all of the collected information for evaluation for up to five years. The Director may approve an extended period in accordance with paragraph B.5 below. Intentionally collected USPI is subject to paragraph B.1 above, and information obtained from a special circumstances collection is subject to paragraph B.4 below, and not this paragraph.

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

4. Special circumstances. If a Component conducts a special circumstances collection under paragraph III.C, the Component may retain the information for evaluation for up to five years. The Director may approve an extended period in accordance with paragraph 5 below.

5. Extended retention

   a. General requirement. The Director may approve, either at the time of collection or thereafter, the further retention of specific information or categories of information subject to paragraphs B1 through 4 above for no more than five years beyond the time permitted in those paragraphs. The Director must find that the extension is necessary to carry out an authorized mission of the Component; find that the Component will retain and handle the information in a manner consistent with the protection of privacy and civil liberties; consider the need for enhanced protections, such as those described in paragraph F; and consult with appropriate legal, privacy, and civil liberties officials. In determining whether to approve an extended retention period, the Director must also find that the information is likely to contain valuable

information that the Component is authorized to collect. The Director must document compliance with the requirements of this paragraph in writing. Any further extension of temporary retention beyond the time specified in this paragraph requires an amendment to these Procedures.

b. Additional requirement for certain communications. In addition to complying with paragraph a above, should a DOE Intelligence Component wish to retain telephone or electronic communications subject to section 309 of the 2015 Intelligence Authorization Act for more than five years, the Component must also comply with the requirements of section 309(b)(3)(B) of that Act.

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 a Component cannot decrypt or understand in the original format. To the extent practicable, unintelligible information will be processed into an intelligible form.

7. Deletion of information. Unless the Component determines that the information covered by paragraphs B.1 through 6 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 the Component's automated systems and all paper files destroyed by the end of the applicable retention period.

C. INFORMATION DISSEMINATED BY ANOTHER COMPONENT OR IC ELEMENT. If another Component or element of the IC disseminates information that may contain USPI to a DOE Intelligence Component, the Component may only retain the information and evaluate it for permanent retention under paragraph D below for as long as the originating agency may retain it, if that period is reported by the originating agency or can be determined by technical reference, or otherwise for a reasonable period not to exceed 5 years. If the other Component or element has already determined that the information meets Attorney General-approved standards for permanent retention, then the recipient Component must only verify that the information is reasonably believed to be necessary for the performance of the recipient's authorized intelligence mission in order to retain the information permanently.

D. PERMANENT RETENTION.[1]

1. Retention standard. A DOE Intelligence Component may permanently retain USPI if 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 the Component by another Component or element of the IC, and determined at the time of collection or subsequently during temporary retention to meet the collection criteria in section III.A;

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

[1] 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 DOE's applicable records retention policies.

or counterintelligence. USPI that is collected in the administration of the Foreign Visitors and Assignments Program and the Foreign Travel Management System or successor programs may be presumed to be necessary to understand or assess foreign intelligence or counterintelligence;

c. The information is retained for purposes of oversight, accountability, or redress. A DOE Intelligence Component will promptly delete information that is retained under this paragraph beyond the period permitted by subsection 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, for so long as such retention is required.

2. Retention of specific USPI. A DOE Intelligence Component 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.

E. GENERAL PROTECTIONS FOR USPI

1. Responsibilities of components. For all USPI, a DOE Intelligence Component 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 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 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 and recording the reason for retaining the data and the authority approving 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 the Office of Intelligence and Counterintelligence.

2. Marking electronic and paper files. Upon issuance of DNI policy, DOE Intelligence Components will use reasonable measures to design and develop information systems to identify and mark or tag files (including emails and attachments) 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, DOE Intelligence Components 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, Components may use a banner informing users prior to access that they may encounter USPI.

3. Reviews. Oversight personnel designated by the Director or a designee will periodically review DOE Intelligence Components' practices for protecting USPI in accordance with these Procedures.

F. ENHANCED SAFEGUARDS

1. Need for enhanced safeguards. Whenever there is a collection involving special circumstances under section III.C, the head of the DOE Intelligence Component or a designee will assess whether there is a need for enhanced safeguards to protect USPI. This assessment will consider:

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

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

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

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

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

f. Practical and technical difficulties associated with implementing any 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 Director.

2. Implementation of enhanced safeguards. If the head of a DOE Intelligence Component or a designee determines that there is a need for enhanced safeguards, that official will consider, and identify for implementation, any of the following protections as deemed appropriate:

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

b. Procedures to restrict access or dissemination, including limiting the number of personnel with access or authority to search; establishing a requirement for higher-level approval 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. Additional training requirements.

f. Additional protective retention measures.

3. Maintenance and disposition of information. The maintenance and disposition of USPI that is retained in the files of the DOE Intelligence Components will conform to this section and to the Component records management schedules approved by the Archivist of the United States for the files or records in which the information is retained.

G. RETENTION FOR BACKUP PURPOSES. Notwithstanding the other provisions of this section, a DOE Intelligence Component 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 a Component 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 a DOE Intelligence Component. Information may be disseminated under this section only if it was properly collected or retained under these Procedures. Within a DOE Intelligence Component, 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 physical and electronic files and information a Component places in databases or on web sites or shared repositories accessible to other persons or organizations outside the Component. 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, 5 USC. § 552a, other applicable laws, and permitted by any enhanced safeguards implemented under paragraph V.F.2.

C. CRITERIA FOR DISSEMINATION. Subject to subsections D through G below, USPI may only be disseminated by employees of DOE Intelligence Components 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 a US person who has 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 DOE (including a DOE contractor) 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 for foreign intelligence, CI, security, law enforcement, cybersecurity, humanitarian assistance, disaster relief, threats to safety, or protective purposes, the DOE Intelligence Component head or delegee must approve the dissemination.

5. Assistance to a DOE Intelligence Component. The dissemination is to a governmental entity, an international entity, or an individual or entity not part of a government and is necessary for the limited purpose of assisting the Component in carrying out an authorized function. For example, a Component may need assistance in decrypting, translating, or analyzing the information. For such a dissemination, the Component will inform the recipient that (i) it should only use the information 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 the Component.

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 Director 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.

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 DOE Inspector General, or to an appropriate congressional oversight committee in accordance with DOE policy and guidance.

D. DISSEMINATIONS TO FOREIGN GOVERNMENTS OR ENTITIES. For any dissemination of USPI to a foreign government or entity, the Director or a designee must find that the disclosure is consistent with applicable international agreements 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

E. DISSEMINATIONS OF LARGE AMOUNTS OF UNEVALUATED USPI. If a DOE Intelligence Component wishes to disseminate a large amount of USPI under paragraphs C.4 through C.6 that has not been evaluated to determine whether it meets the standard for permanent retention, the head of the Component or a single designee must approve the dissemination,

after consulting with the National Security Division of the Department of Justice and the ODNI. The approving official must find that the dissemination complies with the other requirements of this section and that it is not reasonably possible 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 subsections V.E and F, 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.

F. CONTENT OF DISSEMINATIONS. To the extent practicable, a DOE Intelligence Component should not include USPI in a dissemination (other than a dissemination under paragraph C.1 through C.3 above) if the pertinent information can be conveyed in an understandable way without including the identifying information. If a dissemination includes USPI, the disseminating Component will notify the recipient so the recipient can protect the USPI appropriately.

G. IMPROPER DISSEMINATION OF USPI. DOE Intelligence Components will develop policies to address the circumstance when USPI has been disseminated by a Component in error, and when a Component has disseminated information that it originally believed was not USPI but that it later learned was USPI.

H. DISSEMINATION NOT CONFORMING TO THIS SECTION. Any proposed dissemination that does not conform to the requirements of this section must be approved by the legal office responsible for advising the DOE Intelligence Component after consulting with the National Security Division of the Department of Justice and DOE's General Counsel. Such approval will be based on a determination that the proposed dissemination complies with applicable laws, executive orders, and regulations.

VII. PARTICIPATION IN ORGANIZATIONS

A. APPLICABILITY. This section applies to participation by a DOE Intelligence Component or anyone acting on behalf of a Component in any organization in the United States, or in any organization outside the United States that constitutes a US 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). If there is any question about the nature of the participation or whether the person is acting on behalf of a Component, the participant should obtain appropriate guidance.

B. GENERAL DISCLOSURE REQUIREMENT. An employee of a DOE Intelligence Component or anyone acting on behalf of a Component 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 US person, if his or her affiliation with the Component is disclosed to an appropriate official of the organization in accordance with subsection G. Without such disclosure, participation must be permitted by subsections C through E and must be conducted in accordance with subsection F.

C. ACTIVITIES FOR WHICH NO SPECIFIC APPROVAL OR DISCLOSURE IS REQUIRED. No specific approval is required for the following activities:

1. Volunteered information. A DOE Intelligence Component 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 a Component or another element of the IC, the Component may not treat that information as volunteered.

2. Certain activities on the Internet or in other forums. An employee of a DOE Intelligence Component or anyone acting on behalf of a Component 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 a 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 employee of a DOE Intelligence Component or anyone acting on behalf of a Component at commercial classes or training on non-intelligence skills, when under no direction or tasking to collect intelligence, and the true name and DOE or agency 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.

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

7. Seminars and similar events. Participation in 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.

D. MEETINGS OPEN TO THE PUBLIC. In accordance with any DOE or DOE Intelligence Component policy, an official of a Component may approve 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.

E. OTHER UNDISCLOSED PARTICIPATION REQUIRING APPROVAL. Undisclosed participation not falling under the categories provided in subsection C and D may be authorized by the Director, or a designee, after consultation with the Department of Justice, National Security Division.

F. 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 the DOE Intelligence Component, as determined by the head of the Component or a designee.

2. Coordination. The undisclosed participation must be properly coordinated with appropriate agencies in accordance with subsection II.F and any applicable policy and agreements.

3. Collection methods. Participation by a DOE Intelligence Component in an organization in the United States, or in an organization outside the United States that constitutes a US person, is limited to overt collection methods or to collecting publicly available information, unless the activities are carried out under another IC element's authorities in accordance with subsection VIII.A.

4. Compliance with EO 12333. All undisclosed participation must comply with the requirements of section 2.9 of EO 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.

G. MEANS OF DISCLOSURE

1. General. Unless the undisclosed participation is conducted in accordance with subsections C through F, disclosure of the intelligence affiliation of an employee of a DOE Intelligence Component (including anyone else acting on behalf of the Component) 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 the DOE Intelligence Component, *e.g.*, by identifying the particular Component where the name of the Component itself reveals the intelligence affiliation, or by stating the fact of intelligence affiliation where the name does not reveal the underlying affiliation.

2. 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, not affiliated with the IC, in order for the activity of the employee to be disclosed.

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

H. RECORDS. The Director 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. A record of 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 under the authority of another intelligence element in accordance with section VIII.A.

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

A. INTELLIGENCE COLLECTION ACTIVITIES OF OTHER IC ELEMENTS

1. General. DOE Intelligence Components are 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 US laws and be conducted in accordance with procedures approved by the Attorney General. Activities that are beyond the scope of DOE's intelligence authority but within the scope of the requesting element's authority are governed by the intelligence procedures of the requesting element, and must be approved under paragraph 2 below.

2. Collection activities using the authority of another IC element. In order for DOE to provide support or assistance to the foreign intelligence or counterintelligence collection activities of a requesting IC element, using the authorities of the requesting element, the following procedures must be followed:

   a. The request for assistance or support must be in writing from an authorized official of the requesting IC element.

   b. Written assurance must be provided by the requesting element that the activity for which support or assistance is requested is within the authority of the requesting element and will be conducted in accordance with EO 12333, all applicable US laws, other executive orders, Presidential directives, and ICDs. The request must also state that the activity will be conducted in accordance with the procedures of the requesting element approved by the Attorney General, and specifically identify the Attorney General-approved procedures that the DOE personnel will be following.

   c. Written approval of the Director or a designee must be obtained.

   d. Written assurance must be provided by the requesting element that any cooperating DOE employee will not be exposed to any unreasonable or undisclosed risks to his or her health or safety by reason of participation in the intelligence activity for which support is requested.

Approval of DOE support or assistance is to be conditioned upon agreement of the requesting element that all foreign intelligence or counterintelligence information collected with DOE assistance or support using the authorities of the requesting element will be

retained and disseminated only in accordance with the approved intelligence procedures of the requesting element. DOE may condition its support or assistance on agreement by the requesting element to share promptly with DOE, in accordance with the element's procedures, threat information concerning DOE personnel, facilities, and technology.

B. PROVISION OF EXPERT CAPABILITIES TO OTHER IC ELEMENTS

1. General. EO 12333 recognizes DOE's unique technical capabilities. Provision of expert scientific, technical, analytic, and research assistance is expressly authorized in section 1.12(a) of the Executive Order, and DOE may provide it in accordance with DOE policy. Analytic assistance may include the evaluation of "raw" 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 DOE or contractor personnel will facilitate the US intelligence effort, and includes the provision of devices and training.

   All assistance must comply with all applicable US laws and be conducted in accordance with procedures approved by the Attorney General. Assistance that is beyond the scope of DOE's intelligence authority but within the scope of the requesting element's authority is governed by the intelligence procedures of the requesting element, and must be approved under subsection 2 below.

2. Assistance using the authority of another IC element. For DOE to provide assistance to a requesting IC element using the authorities of the requesting element, the following procedures must be followed:

   a. The request for assistance must be in writing from an authorized official of the IC element.

   b. Written assurance must be provided by the requesting element that the activity for which support or assistance is requested is within the authority of the requesting element and will be conducted in accordance with EO 12333, all applicable US laws, other executive orders, Presidential directives, and ICDs. The request must also state that the activity will be conducted in accordance with the procedures of the requesting element approved by the Attorney General, and specifically identify the Attorney General-approved procedures that the DOE personnel will be following.

   c. Written approval of the Director or a designee must be obtained.

   d. Written assurance must be provided by the requesting element that any DOE employee will not be exposed to any unreasonable or undisclosed risks to his or her health or safety as a result of providing the assistance requested.

C. ASSISTANCE TO LAW ENFORCEMENT AGENCIES. Consistent with the limitations of EO 12333, applicable laws, other executive orders, Presidential directives and these Procedures, DOE Intelligence Components are authorized to cooperate with law enforcement authorities as follows:

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

2. Unless otherwise precluded by law or EO 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 Director and the General Counsel of DOE;

4. To provide assistance to law enforcement agencies and security services of foreign governments or international organizations in accordance with established policy. Included in this category are credibility assessments of threatened nuclear incidents; and

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

DOE Intelligence Components may not assist or participate in activities undertaken against US persons that would not be permitted under EO 12333.

IX. CONTRACTING FOR GOODS AND SERVICES

A. GENERAL. This section applies to contracting or other arrangements with US or foreign persons or entities for the procurement of goods and services, including research and development, by DOE Intelligence Components within the United States. It does not apply to contracting with government entities.

B. PROCEDURES

1. Contracts with academic institutions. A DOE Intelligence Component may directly or indirectly enter into a contract or other arrangement for goods or services with an academic institution only if, prior to contracting, the Intelligence Component has disclosed to appropriate officials of the academic institution the fact of sponsorship by the Intelligence Component.

2. Contracts with commercial entities, private institutions, and individuals. A DOE Intelligence Component may directly or indirectly enter into contracts or other arrangements for goods or services, including research and development, with commercial entities, private institutions, and individuals without revealing the sponsorship by the Intelligence Component if:

   a. The contract or other arrangement is for published, publicly available material or for routine goods or services necessary for the support of approved activities, such as credit cards, car rentals, travel, lodging, meals, rental of office space or apartments, and other items incident to approved activities; or

   b. There is a written determination by the Director or a single designee that the sponsorship of the DOE Intelligence Component must be concealed to protect the activity concerned. The Director will identify a legal or oversight official to maintain a record of such determinations.

X. EMPLOYEE CONDUCT

A. GENERAL. DOE employees shall conduct intelligence activities only in accordance with EO 12333, applicable laws, other executive orders, Presidential directives, DOE policy, and these Procedures when acting on behalf of a DOE Intelligence Component, and the applicable procedures of another IC element when acting on behalf of that IC element in response to a tasking.

B. FAMILIARITY WITH RESTRICTIONS

1. Each DOE Intelligence Component shall familiarize its personnel with the provisions of EO 12333, these Procedures, and any instructions implementing these Procedures that apply to its activities.

2. The Director 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 HEADS OF DOE INTELLIGENCE COMPONENTS. The heads of DOE Intelligence Components shall:

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

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

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

4. Ensure that, to the extent permitted by law, legal, oversight, privacy, and civil liberties officials and the Inspector General have access to all information concerning the intelligence activities of that Component necessary to perform their oversight responsibilities.

5. Ensure that employees cooperate fully with the Intelligence Oversight Board (IOB) and its representatives.

XI. OVERSIGHT REPORTING

A. GENERAL. EO 13462 establishes the Intelligence Oversight Board (IOB) in order to enhance the security of the United States by assuring the legality of the activities of the IC. This section addresses the requirements for reporting of questionable intelligence activities. All employees and contractors of DOE will cooperate fully with the IOB.

B. QUESTIONABLE INTELLIGENCE ACTIVITIES

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

2. Identification

a. Each employee of a DOE Intelligence Component must report any questionable intelligence activity to the Director or a designee and to an appropriate oversight official.

b. The head of a DOE Intelligence Component must report any questionable intelligence activity within the Component to the Director 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 the component concerned, or from other DOE 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 DOE policy.

4. Reporting. The Director will report questionable intelligence activities to the IOB to the extent required by section 1.6(c) of EO 12333; EO 13462; and criteria issued by the IOB.[2] To the extent permitted by law, the Director will also provide the IOB with all information necessary to carry out its responsibilities. The Director will provide a copy of all reports to the DNI.

C. REPORTING TO THE ATTORNEY GENERAL. All reports made under subsection B above that involve a possible violation of federal criminal law will be sent to the Attorney General in accordance with the procedures adopted under section 1.6(b) of EO 12333.

XII. GENERAL PROVISIONS

A. ACTIVITIES CONDUCTED FOR ADMINISTRATIVE PURPOSES. A DOE Intelligence Component may collect USPI for administrative purposes. Information is collected for administrative purposes when it is necessary for the administration of a Component but is not collected directly for intelligence purposes. Examples of information collected for administrative purposes include information about systems administration, contracting, public

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

affairs and legislative matters, personnel and training records, and training materials. Nothing in these Procedures prohibits the collection, retention, or dissemination of such information by a Component authorized to engage in such functions.

B. DELEGATION. When these Procedures require a specific DOE 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 DOE policy, unless specifically limited to a single designee.

C. INTERPRETATION. The Director, together with legal counsel, will consult with the Assistant Attorney General for National Security and the ODNI regarding any novel or significant interpretations of these Procedures.

D. DEPARTURES. The Director and the Assistant Attorney General for National Security, after consultation with the 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 Director or the Director's senior representative present may approve a departure from these Procedures. Legal counsel and the Director will be notified as soon as possible. The Director 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. TRANSITION. DOE Intelligence Components will implement these Procedures in accordance with guidance from the Director and will have 18 months from the effective date of these Procedures to implement the requirements of section V and 6 months to implement other requirements.

F. EFFECT. These Procedures are set forth solely for the purpose of internal DOE 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.

XIII. DEFINITIONS

The following definitions apply to these Procedures:

1. Collection. Information is "collected" when it is received by a DOE Intelligence Component, whether or not it is retained by the Component for intelligence or other purposes. Collected information includes information obtained or acquired by any means, including information that is volunteered to the Component. Collected information does not include (i) information that only momentarily passes through a computer system of the Component; (ii) information on the Internet or in an electronic forum or repository outside the Component that is simply viewed or accessed by a Component employee but is not copied, saved, supplemented, or used in some manner; (iii) information disseminated by other DOE Intelligence Components

or IC elements; or (iv) information that is maintained on behalf of another U.S. Government agency and to which the Component does not have access for intelligence purposes.

2. Consent means an agreement by a person or organization to permit a DOE Intelligence Component to take particular actions affecting that person or organization. Consent should be in written or electronic form but may be given orally, unless a specific form of consent is required by law or a particular provision of these Procedures. Consent may be implied if adequate notice is provided that a particular action carries with it the presumption of consent to an accompanying action. For example, appropriate visible posted notices on Government property would carry with them the presumption of consent to a search of briefcases or other property. Similarly, logging on to a computer with an appropriate banner would carry with it the presumption of consent to monitoring of the user's activities on that computer. Consent may also be implied where adequate policy has been published or otherwise articulated. Legal counsel will determine whether a notice or policy is adequate and lawful before the Component relies on the implied consent to take or refrain from taking an action on the basis of the consent.

3. 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.

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

5. DOE Intelligence Components has the meaning given it in subsection I.B.

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

7. 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.

8. Employee, when referring to a DOE employee, means any person employed by DOE; any person employed by another agency and working under the direction and control of DOE; or an employee of a DOE contractor or subcontractor. A source is not an employee.

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

10. 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 US 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 US persons;

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

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

50 USC § 1801(a).

11. 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.

12. Incidental collection of USPI. Collection of USPI is incidental when that USPI is not deliberately sought by a DOE Intelligence Component, but 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.

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

14. Intelligence Community and elements of the IC mean those agencies and elements described in section 3.5(h) of EO 12333.

15. Intentional collection of USPI. Collection of USPI is intentional when that USPI is deliberately sought by a DOE Intelligence Component.

16. International terrorism and international terrorist activities mean 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. 50 USC § 1801(c).

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

18. Organization for purposes of section VII 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.

19. Organization in the United States means an organization physically located in the the United States, whether or not it constitutes a US 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.

20. Overt collection means collection that is openly acknowledged by or is readily attributable to the US Government, or that would be acknowledged in response to an express inquiry. Acknowledgment may include advising of US Government affiliation (confirming the collector's affiliation with an intelligence element is not required, so long as US 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, a DOE intelligence component might monitor Government-furnished equipment based on notice to the individuals from whom the information is collected, but the component would not need to provide the details of the monitoring, or acknowledge which specific users it had chosen to monitor. Similarly, a component might conduct physical surveillance at a DOE facility based on notice to component employees, but it would not need to notify a particular employee that he or she was the subject of the surveillance.

21. 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.

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

Participation on behalf of the Component may also occur when a person acts, on his or her own initiative, for the benefit of the Component. If a source voluntarily furnishes information directly or indirectly to the Component that he or she obtained by participating in an organization, but was not given prior direction or tasking by the Component to join or become a member, collect information, or take that specific action, then that specific action is not on behalf of the Component.

23. Physical surveillance. The deliberate observation by an employee of a DOE Intelligence Component of a person on either a limited or continuous basis, in areas where there is no reasonable expectation of privacy. As part of physical surveillance, an employee may operate surveillance enhancement devices, provided that the devices do not collect information in which a person has a reasonable expectation of privacy. Binoculars, hand-held cameras, and remotely-operated, continuously-monitored cameras are examples of such devices.

    Physical surveillance does not include electronic surveillance or a physical search. It also does not include casual observation, which should be short in duration and narrow in scope. When determining whether an activity is physical surveillance or casual observation, the following factors should be considered:

    a. The duration and frequency of the observation of a particular person or location. The longer or more frequent it is, the more likely it is physical surveillance.

    b. Whether the observation is done from a stationary or moving position, and whether the purpose of moving is limited to obtaining identifying information. Moving for purposes of following a person to ascertain where he or she is going is more likely to be physical surveillance.

    c. Whether the observation is being done with the unaided eye. Aided observation by telephoto lenses or binoculars, particularly for an extended period, is more likely to be physical surveillance.

24. 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.

25. Questionable intelligence activity has the meaning given it in paragraph XI.B.1.

26. Reasonable expectation of privacy means the extent to which a person in particular circumstances has a reasonable belief that his or her activities, property, or communications are private. For example, there is ordinarily a reasonable expectation of privacy in private residences and the content of telephone communications. Some persons may have a reasonable expectation of privacy in certain work spaces. Judicial decisions provide guidance as to whether a person's expectations are reasonable; however, each situation is fact-specific and the law in this area is subject to change.

    A DOE Intelligence Component should consult with legal counsel as to whether a target of physical surveillance or other activity may have a reasonable expectation of privacy in a particular situation.

27. Retention means the maintenance of USPI in either hard copy or electronic format regardless of how the information was collected or how it was disseminated to a DOE Intelligence Component by another Component or element of the Intelligence Community.

28. 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 a single DOE Intelligence Component, or those acting on its behalf, is not a shared repository.

29. Undisclosed participation. Participation by an employee or other person acting on behalf of a DOE Intelligence Component in any organization in the United States, or any organization outside the United States that is a "US person," if the person's intelligence affiliation with a DOE Intelligence Component is not disclosed to an appropriate official of the organization.

30. United States person or US person means any of the following:

    a. A US citizen;

    b. An alien known by the DOE Intelligence Component concerned to be a permanent resident alien;

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

    d. A corporation incorporated in the United States, except for a corporation directed or 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 program or activities in the United States, the membership of the entire international organization will be considered in determining whether it is substantially composed of US persons. If, however, the US-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 US persons.

    Unless specific information to the contrary is obtained, a person or organization in the United States is presumed to be a US 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-US person.

31. US person information (USPI) is information that is reasonably likely to identify one or more specific US 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 US persons. Determining whether information is reasonably likely to identify one or more specific US 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 US person.

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

Ernest Moniz
Secretary of Energy

Loretta E. Lynch
Attorney General

January 9, 2017
Date

17 January 2017
Date