Signals Intelligence Activities

I. These procedures implementing the privacy and civil liberties safeguards in Executive Order 14086 ("these implementing procedures") establish principles that govern how CIA conducts signals intelligence activities and implements certain safeguards for those activities. The United States collects signals intelligence so that its national security decision-makers have access to the timely, accurate, and insightful information necessary to advance the national security interests of the United States and to protect its citizens and the citizens of its allies and partners from harm. Signals intelligence capabilities are a major reason we have been able to adapt to a dynamic and challenging security environment, and the United States must preserve and continue to develop robust and technologically advanced signals intelligence capabilities to protect our security and that of our allies and partners. At the same time, the United States recognizes that signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.

A. Definitions

- **Agency Personnel** - For the purpose of these implementing procedures, staff personnel and non-staff personnel, as defined in Agency issuances; independent contractors; and industrial contractor personnel.
- **Appropriate Remediation** - As defined in Executive Order 14086.
- **Bulk Collection** - As defined in Executive Order 14086.
- **Intelligence** - As defined in Executive Order 12333.
- **Intelligence Community** and **Elements of the Intelligence Community** - As defined in Executive Order 12333.
- **National Security** - As defined in Executive Order 13526.
- **Non-United States Person** - As defined in Executive Order 14086.
- **Personnel of the United States or of its allies or partners** - As defined in Executive Order 14086.
- **Protection of Intelligence Sources and Methods** - Shall have the same meaning as it has in Intelligence Community Directive (ICD) 126.
- **Qualifying Complaint** - As defined in Executive Order 14086.
- **Significant Incident of Non-compliance** - As defined in Executive Order 14086.
- **United States Person** - As defined in Executive Order 12333.
- **Validated Intelligence Priority** - As defined in Executive Order 14086.
- **Weapons of Mass Destruction** - As defined in Executive Order 13526.

II. POLICY

A. Principles. Signals intelligence activities[1] shall be authorized and conducted consistent with the following principles.

1. *Authorized and undertaken in accordance with law*. Signals intelligence activities shall be authorized by statute or by Executive Order, proclamation, or other Presidential directive and undertaken in accordance with the Constitution and with applicable statutes and Executive Orders, proclamations, and other Presidential directives.

2. *Privacy and civil liberties safeguards*. Signals intelligence activities shall be subject to appropriate safeguards, which shall ensure that privacy and civil liberties are integral considerations in the planning and implementation of such activities so that:

   a. Signals intelligence activities shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; and

   b. Signals intelligence activities shall be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

3. *Rigorous oversight*. Signals intelligence activities shall be subjected to rigorous oversight in order to ensure that they comport with the principles identified above.

B. Objectives. Signals intelligence collection activities shall be conducted in pursuit of legitimate objectives.

1. *Legitimate objectives*. Signals intelligence collection activities shall be conducted only in pursuit of one or more of the following objectives:

   a. Understanding or assessing the capabilities, intentions, or activities of a foreign government, a foreign military, a faction of a foreign nation, a foreign-based political organization, or an entity acting on behalf of or controlled by any such foreign government, military, faction, or political organization, in order to protect the national security of the United States and of its allies and partners;

[1] For the purposes of these implementing procedures, as a matter of policy CIA has determined that references to signals intelligence and signals intelligence activities also apply to activities conducted under Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended.

b. Understanding or assessing the capabilities, intentions, or activities of foreign organizations, including international terrorist organizations, that pose a current or potential threat to the national security of the United States or of its allies or partners;

c. Understanding or assessing transnational threats that impact global security, including climate and other ecological change, public health risks, humanitarian threats, political instability, and geographic rivalry;

d. Protecting against foreign military capabilities and activities;

e. Protecting against terrorism, the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person;

f. Protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

g. Protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies and threats conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

h. Protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person;

i. Protecting against threats to the personnel of the United States or of its allies or partners;

j. Protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other objectives identified in subsection II.B.1 of these implementing procedures;

k. Protecting the integrity of elections and political processes, government property, and United States infrastructure (both physical and electronic) from activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person; and

l. Advancing collection or operational capabilities or activities in order to further a legitimate objective identified in subsection II.B.1 of these implementing procedures.

CIA signals intelligence collection activities shall be conducted in pursuit of the legitimate objectives described above, subject to any updates approved by the President. The President may authorize updates to the list of objectives in light of new national security imperatives, such as new or heightened threats to the national security of the United States, for which the President determines that signals intelligence collection activities may be used. The Director of National Intelligence (DNI) shall publicly release any updates to the list of objectives authorized by the President, unless the President determines that doing so would pose a risk to the national security of the United States.

2. *Prohibited objectives*. Signals intelligence collection activities shall not be conducted for the purpose of:

   a. Suppressing or burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press;

   b. Suppressing or restricting legitimate privacy interests;

   c. Suppressing or restricting a right to legal counsel; or

   d. Disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion.

   It is not a legitimate objective to collect foreign private commercial information or trade secrets to afford a competitive advantage to United States companies and United States business sectors commercially. The collection of such information is authorized only to protect the national security of the United States or of its allies or partners.

3. *Validation of signals intelligence collection priorities*. Under section 102A of the National Security Act of 1947, the DNI must establish priorities for the Intelligence Community (IC) to ensure the timely and effective collection of national intelligence, including national intelligence collected through signals intelligence. The DNI does this through the National Intelligence Priorities Framework (NIPF), which the DNI maintains and presents to the President, through the Assistant to the President for National Security Affairs (APNSA), on a regular basis.

   a. NIPF annual review. The CIA, as a participant in the policy processes for establishing signals intelligence collection priorities and requirements, shall, on an annual basis, review any priorities and requirements identified by the Agency and advise the DNI whether each should be maintained, with a copy of the advice provided to the APNSA.

   b. Civil Liberties Protection Officer (CLPO) assessment. In order to ensure that signals intelligence collection activities are undertaken to advance legitimate objectives, before presenting the NIPF or any successor framework that

identifies intelligence priorities to the President, the DNI shall obtain from the CLPO of the Office of the Director of National Intelligence (ODNI) an assessment as to whether, with regard to anticipated signals intelligence collection activities, each of the intelligence priorities identified in the NIPF or successor framework:

(1) Advances one or more of the legitimate objectives set forth in subsection II.B.1 of these implementing procedures;

(2) Neither was designed nor is anticipated to result in signals intelligence collection in contravention of the prohibited objectives set forth in subsection II.B.2 of these implementing procedures; and

(3) Was established after appropriate consideration for the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

c. DNI review. If the DNI disagrees with any aspect of the CLPO's assessment with respect to any of the intelligence priorities identified in the NIPF or successor framework, the DNI shall include the CLPO's assessment and the DNI's views when presenting the NIPF to the President.

C. Privacy and Civil Liberties Safeguards. The following safeguards shall fulfill the principles contained in subsection II.A.2-3 of these implementing procedures.

1. Collection of signals intelligence.

a. The United States shall conduct signals intelligence collection activities only following a determination that a specific signals intelligence collection activity, based on a reasonable assessment of all relevant factors, is necessary to advance a validated intelligence priority, although signals intelligence does not have to be the sole means available or used for advancing aspects of the validated intelligence priority; it could be used, for example, to ensure alternative pathways for validation or for maintaining reliable access to the same information. In determining whether to collect signals intelligence consistent with this principle, the United States—through CIA or through an interagency committee consisting in whole or in part of the heads of elements of the IC, the heads of departments containing such elements, or their designees—shall consider the availability, feasibility, and appropriateness of other less intrusive sources and methods for collecting the information necessary to advance a validated intelligence priority, including from diplomatic and public sources, and shall prioritize such available, feasible, and appropriate alternatives to signals intelligence.

b. Signals intelligence collection activities shall be as tailored as feasible to advance a validated intelligence priority and, taking due account of relevant

factors, not disproportionately impact privacy and civil liberties. Such factors may include, depending on the circumstances, the nature of the pursued objective; the feasible steps taken to limit the scope of the collection to the authorized purpose; the intrusiveness of the collection activity, including its duration; the probable contribution of the collection to the objective pursued; the reasonably foreseeable consequences to individuals, including unintended third parties; the nature and sensitivity of the data to be collected; and the safeguards afforded to the information collected.

c. Scope. For purposes of subsection II.C.1 of these implementing procedures, the scope of a specific signals intelligence collection activity may include, for example, a specific line of effort or target, as appropriate. Before conducting signals intelligence collection activities that raise potential heightened policy sensitivities, CIA components shall coordinate with the Privacy and Civil Liberties Officer (PCLO) and the Chief Operating Officer to determine whether additional approvals or civil liberties protections are needed to ensure that collection is necessary and proportionate to a legitimate objective.

2. Bulk collection of signals intelligence.

a. Targeted collection. In order to minimize any impact on privacy and civil liberties, a targeted signals intelligence collection activity that temporarily uses data acquired without discriminants (for example, without specific identifiers or selection terms) shall be subject to the safeguards described in subsection II.C.2 of these implementing procedures, unless such data is:

(1) Used only to support the initial technical phase of the targeted signals intelligence collection activity;

(2) Retained for only the short period of time required to complete this phase; and

(3) Thereafter deleted.

b. Bulk collection. Targeted collection shall be prioritized. The bulk collection of signals intelligence shall be authorized only based on a determination—by CIA or through an interagency committee consisting in whole or in part of the heads of elements of the IC, the heads of departments containing such elements, or their designees—that the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection. When it is determined to be necessary to engage in bulk collection in order to advance a validated intelligence priority, the CIA shall apply reasonable methods and technical measures in order to limit the data collected and retained to only what is necessary to advance a validated intelligence priority, while minimizing the collection and retention of non-pertinent information.

c. Uses of bulk collection. The CIA shall use signals intelligence collected through bulk collection only in pursuit of one or more of the following objectives:

(1) Protecting against terrorism, the taking of hostages, and the holding of individuals captive (including the identification, location, and rescue of hostages and captives) conducted by or on behalf of a foreign government, foreign organization, or foreign person;

(2) Protecting against espionage, sabotage, assassination, or other intelligence activities conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(3) Protecting against threats from the development, possession, or proliferation of weapons of mass destruction or related technologies and threats conducted by, on behalf of, or with the assistance of a foreign government, foreign organization, or foreign person;

(4) Protecting against cybersecurity threats created or exploited by, or malicious cyber activities conducted by or on behalf of, a foreign government, foreign organization, or foreign person;

(5) Protecting against threats to the personnel of the United States or of its allies or partners; and

(6) Protecting against transnational criminal threats, including illicit finance and sanctions evasion related to one or more of the other objectives identified in subsection II.C.2.c of these implementing procedures.

d. Queries of bulk collection. Agency personnel shall conduct queries of unminimized signals intelligence obtained by bulk collection consistent with the permissible uses of signals intelligence obtained by bulk collection identified above and according to policies and procedures issued under these implementing procedures, which shall appropriately take into account the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.

3. *Queries of signals intelligence*.

Agency personnel querying databases containing information obtained through signals intelligence activities shall structure query terms and techniques in a manner reasonably designed to identify intelligence relevant to an authorized intelligence requirement and minimize the review of personal information not relevant to an authorized intelligence requirement.

D. Handling of Personal Information Collected Through Signals Intelligence

1. *Minimization*. The CIA shall apply policies and procedures designed to minimize the dissemination and retention of personal information collected through signals intelligence.

   a. Dissemination. The CIA:

      (1) Shall disseminate non-United States persons' personal information collected through signals intelligence only if it involves one or more of the comparable types of information that section 2.3 of Executive Order 12333 and the CIA's implementing Attorney General Guidelines state may be disseminated in the case of information concerning United States persons;

      (2) Shall not disseminate personal information collected through signal intelligence solely because of a person's nationality or country of residence;

      (3) Shall disseminate within the United States Government personal information collected through signals intelligence only if an authorized and appropriately trained individual has a reasonable belief that the personal information will be appropriately protected and that the recipient has a need to know the information;

      (4) Shall take due account of the purpose of the dissemination, the nature and extent of the personal information being disseminated, and the potential for harmful impact on the person or persons concerned before disseminating personal information collected through signals intelligence to recipients outside the United States Government, including to a foreign government or international organization; and

      (5) Shall not disseminate personal information collected through signals intelligence for the purpose of circumventing the provisions of this order.

   b. Retention. The CIA:

      (1) Shall retain non-United States persons' personal information collected through signals intelligence only if it involves one or more of the comparable types of information that section 2.3 of Executive Order 12333 and the CIA's implementing Attorney General Guidelines state may be retained in the case of information concerning United States persons and shall subject such information to the same retention periods that would apply to comparable information concerning United States persons;

      (2) Shall subject non-United States persons' personal information collected through signals intelligence for which no final retention determination has

been made to the same temporary retention periods that would apply to comparable information concerning United States persons; and

(3) Shall delete non-United States persons' personal information collected through signals intelligence that may no longer be retained in the same manner that comparable information concerning United States persons would be deleted.

2. *Data security and access*. The CIA:

a. Shall process and store personal information collected through signals intelligence under conditions that provide appropriate protection and prevent access by unauthorized persons, consistent with the applicable safeguards for sensitive information contained in relevant Executive Orders, proclamations, other Presidential directives, Intelligence Community Directives, and associated policies;

b. Shall limit access to such personal information to authorized Agency personnel who have a need to know the information to perform their mission and have received appropriate training on the requirements of applicable United States law, as described in policies and procedures issued under these implementing procedures; and

c. Shall ensure that personal information collected through signals intelligence for which no final retention determination has been made is accessed only in order to make or support such a determination or to conduct authorized administrative, testing, development, security, or oversight functions.

3. *Data quality*. The CIA shall include personal information collected through signals intelligence in intelligence products only as consistent with applicable Intelligence Community Standards for accuracy and objectivity, including Intelligence Community Directive (ICD) 203, *Analytic Standards*, with a focus on applying standards relating to the quality and reliability of the information, consideration of alternative sources of information and interpretations of data, and objectivity in performing analysis.

4. *Documentation*. In order to facilitate the oversight processes set forth in subsection II.E of these implementing procedures and the redress mechanism set forth in these implementing procedures, the CIA shall maintain documentation of signals intelligence collection activities to the extent reasonable in light of the nature and type of collection at issue and the context in which it is collected. The content of any such documentation may vary based on the circumstances but shall, to the extent reasonable, provide the factual basis pursuant to which the CIA, based on a reasonable assessment of all relevant factors, assesses that the signals intelligence collection activity is necessary to advance a validated intelligence priority.

E. Subjecting Signals Intelligence Activities to Rigorous Oversight. The actions directed in this subsection are designed to build on the oversight mechanisms that the CIA already has in place, in order to further ensure that signals intelligence activities are subjected to rigorous oversight.

1. *Legal, oversight, data privacy, cybersecurity, and compliance officials*. The CIA:

   a. Shall have in place senior-level legal, oversight, data privacy, cybersecurity, and compliance officials who conduct periodic oversight of signals intelligence activities, including an Inspector General, a Privacy and Civil Liberties Officer (PCLO), and an officer or officers in a designated compliance role with the authority to conduct oversight of and ensure compliance with applicable United States law;

   b. Shall provide such legal, oversight, data privacy, cybersecurity, and compliance officials access to all information pertinent to carrying out their oversight responsibilities under this subsection, consistent with the protection of intelligence sources or methods, including their oversight responsibilities to ensure that any appropriate actions are taken to remediate an incident of non-compliance with applicable United States law; and

   c. Shall not take any actions designed to impede or improperly influence such legal, oversight, data privacy, cybersecurity, and compliance officials in carrying out their oversight responsibilities under this subsection.

2. *Training*. The CIA shall maintain appropriate training requirements to ensure that all Agency personnel with access to signals intelligence know and understand the requirements of these implementing procedures and the guidance, policies, and procedures for notifying and remediating incidents of non-compliance with applicable United States law.

3. *Incidents of non-compliance*.

   a. Notification. All Agency personnel shall report potential incidents of non-compliance to the PCLO. The PCLO, in coordination with the Office of General Counsel (OGC), shall promptly report incidents of non-compliance to the CDO and relevant components to ensure their remediation, and shall promptly report significant incidents of non-compliance to the Director of the CIA (D/CIA) and the Director of National Intelligence (DNI), and, where appropriate, to the Department of Justice (DOJ) and the Foreign Intelligence Surveillance Court.

   b. Remediation. Upon receipt of such notification, the D/CIA, through the CIA PCLO, and the DNI shall ensure that any necessary actions are taken to remediate and prevent the recurrence of the significant incident of non-compliance, which may include notifying other agencies.

F. Redress Mechanism

1. *CIA assistance*. The CIA shall provide the ODNI CLPO with access to information necessary to conduct the reviews described in Section 3(c)(i) or Section 3(d)(i) of Executive Order 14086. This will be done in the most practicable manner that maintains protection of intelligence sources and methods. Protection of intelligence sources and methods shall have the same meaning as it has in Intelligence Community Directive (ICD) 126. The CIA shall not take any actions designed to impede or improperly influence the CLPO's or a Data Protection Review Court (DPRC) panel's reviews.

2. *CIA Privacy and Civil Liberties Officer (PCLO) support*. The CIA PCLO shall support the ODNI CLPO and a DPRC panel as they perform reviews under the redress mechanism.

3. *CIA assistance to Privacy and Civil Liberties Oversight Board (PCLOB)*. The CIA shall provide the PCLOB with access to information necessary for the PCLOB to conduct the annual review of the redress process described in subsection 3(e)(i) of the Executive Order 14086, consistent with the protection of intelligence sources and methods.

4. *Binding effect*. The CIA shall comply with any determination by the ODNI CLPO to undertake appropriate remediation, subject to any contrary determination by a DPRC panel, and shall comply with any determination by a DPRC panel to undertake appropriate remediation under the redress mechanism.

G. Amendment or Departure

1. Except as provided in this subsection, the D/CIA or DD/CIA, or designee, must approve in advance any material amendment to or departure from these procedures. The General Counsel, after consultation with ODNI and the National Security Division (NSD) of DOJ, and the PCLO will advise the D/CIA or DD/CIA, or designee, on requests to amend these procedures.

2. If securing any approval that would otherwise be required is not practical and there is a reasonable belief that:

    a. A person's life or physical safety is in imminent danger, and the information is relevant to the danger or its prevention, reduction, or elimination; or

    b. The time required to secure prior approval would cause failure or delay in obtaining significant intelligence, and such failure or delay would result in substantial harm to national security;

    the most senior CIA official available at the time may approve a departure from these procedures.

3. The D/CIA or DD/CIA, or designee, the General Counsel, and the PCLO will be promptly notified of any such departures as soon thereafter as possible. The General Counsel will provide prompt written notice of any such departures stating why advance approval was not possible and describing the actions taken to ensure activities were conducted lawfully to ODNI and the National Security Division of DOJ. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

III. RESPONSIBILITIES

A. The Director of the Central Intelligence Agency (D/CIA) or designee shall:

1. After consultation with the General Counsel and the Privacy and Civil Liberties Officer (PCLO), approve any extension of the retention period for unevaluated information acquired through signals intelligence collection activities pursuant to the CIA's implementing Attorney General Guidelines.

B. The Deputy Director of the Central Intelligence Agency (DD/CIA) or designee shall:

1. Manage the CIA's participation in the policy processes for reviewing signals intelligence collection priorities and requirements, including sensitive collection activities, and advising the Director of National Intelligence (DNI) and the Assistant to the President for National Security Affairs (APNSA) under subsection II.B.3 of these implementing procedures, and the policy processes for reviewing the permissible uses of bulk signals intelligence under subsection II.C.2.c of these implementing procedures.

C. The Chief Operating Officer (COO) of the Central Intelligence Agency or designee shall:

1. Monitor the implementation of these implementing procedures.

D. The Chief Data Officer (CDO) of the Central Intelligence Agency or designee shall:

1. Establish policies and procedures for the implementation of these implementing procedures, including those regarding:

    a. Queries of unminimized signals intelligence obtained by bulk collection under subsection II.C.2.c of these implementing procedures;

    b. Minimizing the retention of personal information collected through signals intelligence under subsection II.D.1.b of these implementing procedures;

c. Limiting access to personal information to authorized Agency personnel under subsection II.D.2.b of these implementing procedures; and

d. Training under subsection II.E.2 of these implementing procedures;

2. In coordination with the PCLO, conduct periodic oversight and assessments of data standards, guidelines, and procedures for compliance with the legal requirements relating to documentation, handling, and retention of data acquired through signals intelligence activities;

3. Conduct periodic audits of compliance with access and training requirements, and provide results to the PCLO and the relevant components; and

4. Consult with OPCL on incorporating results of oversight, assessments, and audits into training programs.

E. The Inspector General (IG) of the Central Intelligence Agency or designee shall:

1. As part of the IG's statutory responsibilities, conduct audits, inspections, and investigations of CIA programs and operations to determine compliance with applicable laws and regulations.

F. The Deputy Director of the Central Intelligence Agency for Operations (DDO) or designee shall:

1. Establish policies and procedures designed to minimize the dissemination of personal information collected through signals intelligence under subsection II.D.1.a of these implementing procedures.

G. The Privacy and Civil Liberties Officer (PCLO) of the Central Intelligence Agency or designee shall:

1. Provide privacy and civil liberties compliance advice and assistance regarding implementation of these implementing procedures and guidance, policies, and procedures implementing these implementing procedures;

2. In coordination with the CDO, conduct oversight and periodic assessments of personal information acquired through signals intelligence collection activities;

3. Produce privacy and civil liberties reports regarding implementation of these implementing procedures;

4. With the General Counsel, coordinate on requests to extend the retention period for unevaluated information acquired through signals intelligence collection activities pursuant to the CIA's implementing Attorney General Guidelines and monitor

compliance with such extended retention periods by tracking and auditing such extensions;

5. In coordination with the Office of General Counsel (OGC), promptly report incidents of non-compliance to the appropriate officials;

6. Take actions necessary to remediate and prevent the recurrence of significant incidents of non-compliance;

7. Establish, oversee and manage the process by which the CIA records, investigates, and responds to the DNI's review for potential redress following a qualifying claim of improper signals intelligence activities;

8. In coordination with the CDO, conduct periodic oversight and assessments of data standards, guidelines, and procedures for compliance with the legal requirements relating to documentation, handling, and retention of data acquired through signals intelligence activities; and

9. Review the results of CDO audits of compliance with access and training reequipments for privacy and civil liberties interests and notify CDO of any concerns.

H. The Heads of Directorates, Independent Offices, and Mission Centers or designees shall:

1. Ensure appropriate Agency personnel are trained on these implementing procedures and guidance, policies, and procedures established under these implementing procedures;

2. Review signals intelligence collection priorities and requirements identified by the Agency annually and advise the DNI whether each should be maintained;

3. Determine whether signals intelligence activities are necessary to advance a validated intelligence priority and ensure that such activities are conducted in a manner that is proportionate to the validated intelligence priority;

4. Determine whether bulk collection of signals intelligence is necessary to advance a validated intelligence priority because the information cannot reasonably be obtained by targeted collection;

5. Ensure that signals intelligence collection activities are conducted in pursuit of legitimate objectives and are not conducted for the purpose of prohibited objectives;

6. Coordinate with PCLO to determine whether additional approvals or civil liberties protections are needed to ensure that collection is necessary and proportionate to a

legitimate objective before conducting signals intelligence collection activities that raise potential heightened policy sensitivity;

7. Conduct oversight and periodic assessments of signals intelligence activities; and

8. Maintain documentation of signals intelligence collection activities.

I. Agency Personnel shall:

1. Attend training as required by these implementing procedures;

2. Comply with these implementing procedures and any guidance, policies, and procedures established under these implementing procedures;

3. Use and query signals intelligence collected through bulk collection only in pursuit of permissible uses;

4. Structure query terms and techniques in a manner reasonably designed to identify relevant intelligence and minimize the review of non-pertinent information;

5. Retain and disseminate non-United States persons' personal information collected through signals intelligence only if comparable information concerning U.S. persons could be retained or disseminated;

6. Notify the appropriate Head of Directorate, Independent Office, or Mission Center and the Privacy and Civil Liberties Officer of incidents of potential noncompliance; and

7. Cooperate fully with any investigation of improper signals intelligence collection activities and comply with any determination by either the Director of National Intelligence or the Data Protection Review Court to undertake appropriate remediation.