Signals Intelligence Activities

While protecting our nation through the collection of signals intelligence (SIGINT) as authorized by law and policy, the Central Intelligence Agency (CIA), referred to herein as the "Agency," is committed to protecting the personal information of all people regardless of their nationality. This regulation establishes the principles that govern how the CIA conducts SIGINT activities and codifies into formal policy many existing practices which had not been previously put forth in a single regulatory issuance.

Definitions

- **Foreign person** - means a person who does not meet the definition of "United States person" in Executive Order 12333.
- **Intelligence** - has the same meaning as it does in the National Security Act of 1947.
- **Personal information** - covers the same types of information covered by "information concerning U.S. persons" under Section 2.3 of Executive Order 12333.
- **SIGINT collected in bulk** - means the authorized collection of large quantities of signals intelligence data which, due to technical or operations considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.).
- **United States person** - has the same meaning as it does in Executive Order 12333.

General Policy: The Agency shall not collect SIGINT unless authorized to do so by statute or Executive Order, proclamation, or other Presidential directive, and such collection shall be undertaken in accordance with the Constitution and applicable statutes, Executive Orders, proclamations, Presidential directives, Agency regulatory issuances, and implementing guidance.

- Privacy and civil liberties shall be integral considerations in the planning of SIGINT activities. SIGINT shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and CIA missions and not for any other purpose.
- The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially. Certain economic purposes, such as identifying trade or sanctions violations or government influence or direction, shall not constitute competitive advantage.
- SIGINT activities shall be as tailored as feasible. In determining whether to collect SIGINT, the Agency shall consider the availability of other information, including from diplomatic and public sources. Such appropriate and feasible alternatives to SIGINT shall be prioritized by means of the least intrusive technique required to obtain the intelligence of the nature, reliability, and timeliness required.
- The collection, use, retention, and dissemination of information concerning "United States persons" are governed by multiple legal and policy requirements, such as those required by the Foreign Intelligence Surveillance Act of 1978

(FISA), the Privacy Act of 1974, and Executive Order 12333. This regulation is not intended to alter the rules applicable to U.S. persons in FISA, the Privacy Act, Executive Order 12333, or other applicable law.

Collection

Refining the Process for Collecting Signals Intelligence: The Agency shall participate in the United States Government (USG) policy processes for establishing SIGINT collection priorities and requirements.

- PPD-28 provides that the Agency must collect bulk SIGINT in certain circumstances in order to identify new or emerging threats and other vital national security information which is often hidden within the large and complex system of modern global communications. It also recognizes the privacy and civil liberties concerns raised when bulk SIGINT is collected. PPD-28 directs the Intelligence Community (IC) to assess the feasibility of alternatives that would allow the IC to conduct targeted SIGINT collection rather than bulk SIGINT collection. Accordingly, when engaging in SIGINT collection, the Agency should conduct targeted SIGINT collection activities rather than bulk SIGINT collection activities when practicable. SIGINT collection activities should be directed against specific foreign intelligence targets or topics through the use of discriminants (e.g., specific facilities, identifiers, selection terms, etc.) when practicable.
- Agency components shall consult with the Privacy and Civil Liberties Officer (PCLO) and the Executive Director of the Central Intelligence Agency (EXDIR) or their designees on novel or unique SIGINT collection activities, and any significant changes to existing SIGINT collection activities, to ensure that there are appropriate safeguards to protect personal information.
- The Agency shall, on an annual basis, review SIGINT priorities and requirements identified by the Agency and advise the Director of National Intelligence (DNI) whether each should be maintained, with a copy of the advice provided to the Assistant to the President and National Security Advisor (APNSA).

Excluded Activities: The above does not apply to SIGINT activities undertaken by the CIA in support of:

- human intelligence (HUMINT) operations;
- covert action;
- FBI predicated law enforcement investigations other than those conducted solely for purposes of acquiring foreign intelligence; or
- military operations in an area of active hostilities.

Use of SIGINT Collected in Bulk

The Agency shall use SIGINT collected in bulk only for the purposes of detecting or countering:

- espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;
- threats to the United States and its interests from terrorism;
- threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction;
- cybersecurity threats;
- threats to U.S. or allied Armed Forces or other U.S. or allied personnel;
- transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes identified in the section on "Use of SIGINT Collection in Bulk"; and
- any threat to the national security determined to be a permissible use of SIGINT collected in bulk in the review process established by Section 2 of PPD-28, or for any other lawful purpose, when approved by the President.

The Agency shall not use SIGINT collected in bulk for the purpose of:

- suppressing or burdening criticism or dissent;
- disadvantaging persons based upon their ethnicity, race, gender, sexual orientation, or religion;
- affording a competitive advantage to U.S. companies and U.S. business sectors commercially; or
- achieving any other purpose than those identified above.

As provided in footnote 5 of PPD-28, the prohibitions noted immediately above on the use of SIGINT collected in bulk do not apply to SIGINT collected in bulk that is temporarily acquired to facilitate the acquisition of targeted collection.

The Agency shall participate in the policy processes for reviewing the permissible uses of SIGINT collected in bulk.

The Agency shall, on an annual basis, review the Agency's use of SIGINT collected in bulk and advise the DNI and APNSA on recommended additions to or removals from the list of permissible uses of SIGINT collected in bulk.

Systems containing SIGINT collected in bulk shall record sufficient details of queries to enable oversight and compliance with permissible uses of SIGINT collected in bulk, and to enable retention determinations.

Retention and Access

Retention of personal information concerning foreign persons acquired through SIGINT activities is authorized only if the Agency has lawfully collected or received the information in accordance with FISA or Part I of Executive Order 12333 and the processes established by PPD-28, and the retention of comparable information concerning U.S. persons would be permitted under Section 2.3 of Executive Order 12333. Such information shall be subject to the same retention periods as comparable information concerning U.S. persons. Information for which no permanent retention determination has been made shall not be retained for more than five (5) years, unless the DNI expressly determines that continued retention is in the national security interests of the United States. Information for which no permanent retention determination has been made may be retained for up to five (5) years, or the extended period approved by the DNI, to determine whether it falls within one of the following categories that meet the standard for permanent retention:

- information that is publicly available or collected with the consent of the person concerned;
- information constituting foreign intelligence or counterintelligence. If the Agency is permanently retaining personal information concerning a foreign person because it is foreign intelligence, the information must relate to an authorized intelligence requirement, and cannot be retained solely because of the person's foreign status. Thus, for example, personal information about the routine activities of a foreign person may not be retained unless it relates to an authorized foreign intelligence requirement;
- information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation;
- information needed to protect the safety of any persons or organizations, including those who are targets, victims or hostages of international terrorist organizations;
- information needed to protect foreign intelligence or counterintelligence sources, methods and activities from unauthorized disclosure;
- information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;
- information arising out of a lawful personnel, physical or communications security investigation;
- information acquired by overhead reconnaissance not directed at specific U.S. persons;
- incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and
- information necessary for administrative purposes.

Personal information acquired through SIGINT activities for which no determination has been made that it can be permissibly disseminated or retained shall be accessed only in order to make such determinations (or to conduct authorized administrative, security, compliance, and oversight functions).

Adequate protections of personal information shall be provided to prevent unauthorized access, consistent with the applicable safeguards for sensitive information contained in relevant Executive Orders, proclamations, Presidential directives, Intelligence Community Directives (ICDs), and associated policies.

Access to personal information acquired through SIGINT activities shall be limited to authorized and trained personnel, such as personnel responsible for analyzing and processing the information who have a need to know the information in order to perform their mission, consistent with the personnel security requirements of relevant Executive Orders, ICDs, and associated policies.

Personnel will be provided appropriate and adequate training in the principles set forth in this regulation and any associated guidance before being authorized access to unevaluated and unminimized personal information acquired through SIGINT activities. Training is required for those personnel who engage in collection requirements, targeting, or other disciplines that deal with SIGINT collection. Further, administrators and other support personnel who require access to these collections also must be trained prior to being granted access. Failure to obtain or maintain training requirements will result in the loss of access until requirements are met.

Personnel querying databases containing information acquired through SIGINT 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.

Systems containing SIGINT shall record sufficient details of purges to enable oversight and compliance with retention policies.

Dissemination

Dissemination of personal information concerning foreign persons acquired through SIGINT activities is authorized only if the Agency has lawfully collected or received the information in accordance with FISA or Part I of Executive Order 12333 and the processes established by PPD-28, and the dissemination of comparable information concerning U.S. persons would be permitted under Section 2.3 of Executive Order 12333, as listed in the Retention Section above. If the Agency is disseminating personal information concerning a foreign person because it is foreign intelligence, the information must relate to an authorized intelligence requirement, and cannot be disseminated solely because of the person's foreign status. Thus, for example, personal information about the routine activities of a foreign person may not be disseminated unless it relates to an authorized foreign intelligence requirement.

The Agency shall establish policies and procedures reasonably designed to minimize the retention and dissemination of personal information acquired through SIGINT activities.

The Agency shall include personal information in intelligence products and reports only as consistent with applicable IC standards for accuracy and objectivity, and as necessary to meet an analytic or operational purpose, as set forth in relevant IC directives.

When disseminating unevaluated SIGINT that may contain personal information, the Agency will inform the recipient that the dissemination may contain personal information so that the recipient can take appropriate steps to protect that information.

Dissemination of personal information acquired through SIGINT activities to a foreign government is authorized only if the dissemination meets the following criteria:

- the dissemination is in the interests of the United States; and
- the dissemination complies with applicable laws, Executive Orders, and IC policies.

Compliance

Agency policies and procedures shall include appropriate measures to facilitate compliance and oversight of the implementation of safeguards protecting personal information acquired through SIGINT activities, to include periodic auditing against the standards required by this regulation and implementing guidance, and training for personnel authorized to access such information.

Agency information systems will be designed to monitor activity in datasets involving personal information and facilitate the monitoring, recording, and auditing of queries of personal information.

The Agency shall notify personnel how they may securely report violations of law, regulation, or policy.

When a significant compliance issue occurs involving personal information of any person, regardless of nationality, collected as a result of SIGINT activities, the issue shall, in addition to any existing reporting requirements, be reported promptly to the PCLO, who shall determine what, if any, corrective actions are necessary. All significant compliance issues involving personal information shall be promptly reported to the DNI. If the issue involves a foreign person, the DNI, in consultation with the Secretary of State and the Director of the Central Intelligence Agency (D/CIA), shall determine whether steps should be taken to notify the relevant foreign government, consistent with the protection of sources and methods and of U.S. personnel.

Responsibilities

The Director of the Central Intelligence Agency (D/CIA) shall approve any exception to any provision of this regulation that is not required by the Constitution or a statute, Executive Order, proclamation, or Presidential directive, and notify, and if practicable consult in

advance, the ODNI and the National Security Division (NSD) of the Department of Justice (DOJ).

The Deputy Director of Central Intelligence Agency (DD/CIA) or designee shall oversee the annual review of SIGINT priorities and requirements identified by the Agency and advise the D/CIA, for subsequent passage to the DNI and APNSA, on whether such activities should be maintained; manage the Agency's participation in the policy review process for reviewing SIGINT collection activities, to include sensitive SIGINT collection activities and the use of bulk SIGINT.

The Executive Director of the Central Intelligence Agency (EXDIR) or designee shall:

- Establish CIA policies, procedures, and guidance for the implementation of this regulation to include;
  - Training;
  - Limitations on the use of bulk SIGINT;
  - Review of SIGINT collection activities;
  - Procedures to minimize the retention and dissemination of personal information acquired through SIGINT activities; and
  - Other issues, as required;
- In coordination with the Privacy and Civil Liberties Officer (PCLO),
  - Coordinate on novel or unique collection activities, or significant changes to existing collection activities, to ensure that appropriate safeguards are in place to protect personal information acquired through such activities;
  - Establish procedures to receive, evaluate, and report significant compliance incidents for this regulation to the DNI; and
  - Review requests for extended retention of personal information concerning foreign persons acquired through SIGINT activities and advise the DD/CIA and the D/CIA whether they should be transmitted to the DNI;
- Monitor implementation and compliance with the established policies, procedures, and guidance for PPD-28.

The Inspector General shall 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.

The PCLO shall:

- provide compliance advice and assistance regarding the requirements of PPD-28, this regulation, or any additional procedures or guidance for PPD-28;
- coordinate on novel or unique collection activities, or significant changes to existing collection activities, to ensure that appropriate safeguards are in place to protect personal information acquired through such activities;
- conduct periodic oversight and assessments of personal information acquired through SIGINT activities to ensure compliance with privacy and civil liberties;

- advise the D/CIA, the DD/CIA, the EXDIR or an appropriate designee and Heads of Directorates and Independent Offices on the development of:
    - procedures to safeguard personal information acquired through SIGINT activities; and
    - privacy and civil liberties training in support of PPD-28 principles;
- produce privacy and civil liberties reports, in coordination with the affected Directorates and Independent Offices;
- report significant compliance issues involving personal information acquired through SIGINT activities to the D/CIA and DNI; and
- coordinate on requests for extended retention of personal information concerning foreign persons acquired through SIGINT activities for privacy and civil liberties issues.

The Heads of CIA Directorates and Independent Offices shall:

- implement the policies, procedures, and guidance established by this regulation in coordination with the EXDIR or designee;
- provide training to personnel who require access in the performance of their duties to personal information acquired through SIGINT activities in the performance of their duties;
- initiate requests to the EXDIR or designee, in coordination with the PCLO, for extended retention of personal information of foreign persons acquired through SIGINT activities;
- on an annual basis, review SIGINT priorities and requirements identified by respective offices and advise the EXDIR or designee on whether these should be maintained;
- working with the EXDIR or designee, participate in the policy review process for SIGINT activities, to include sensitive SIGINT collection activities and permissible uses of bulk SIGINT;
- assist the EXDIR or designee, IG, and PCLO in conducting oversight and periodic assessments of SIGINT collection activities containing personal information; and
- consult with the EXDIR or designee and PCLO on novel or unique SIGINT collection activities and significant changes to existing SIGINT collection activities, to ensure that appropriate safeguards are in place to protect personal information acquired through such activities.

Agency personnel shall:

- comply with the principles, policies, and procedures of this regulation and any implementing guidance; and
- report compliance issues to the appropriate Head of Directorate or Independent Office and the PCLO.