



**DRUG ENFORCEMENT ADMINISTRATION  
OFFICE OF NATIONAL SECURITY INTELLIGENCE**

**EXECUTIVE ORDER 14086 – POLICY AND PROCEDURE  
POLICY NUMBER 4100  
6/30/2023**

**TABLE OF CONTENTS**

1.0	AUTHORITIES	2
2.0	INTRODUCTION	2
3.0	POLICY AND PROCEDURES	3
4.0	TRAINING	6
5.0	DEVIATIONS FROM THESE PROCEDURES	6
6.0	CONCLUSION	6
7.0	EFFECTIVE DATE/REVISION HISTORY	6
8.0	ACRONYMS	7

## 1.0 AUTHORITIES

- A. [Executive Order \(E.O.\) 14086 Enhancing Safeguards for United States Signals Intelligence Activities](#)
- B. [E.O. 12333 United States Intelligence Activities](#)
- C. [Presidential Policy Directive \(PPD-28\) Signals Intelligence, January 17, 2014](#)
- D. [National Security Act of 1947, as amended](#)
- E. [Intelligence Community Directive \(ICD\) 203, \*Analytic Standards\*](#)

## 2.0 INTRODUCTION

E.O. 14086 bolsters privacy and civil liberty safeguards for U.S. signals intelligence (SIGINT) activities and creates an independent and binding mechanism enabling individuals in qualifying states (defined as countries and regional economic integration organizations), as designated under the E.O., to seek redress through the submission of a qualifying complaint if they believe their personal data was collected through U.S. SIGINT in a manner that violated applicable U.S. law.

Among other provisions, Section 2(c)(iv) of E.O. 14086 requires the head of each element of the Intelligence Community (IC) to: apply relevant policies and procedures issued pursuant to PPD-28, update those policies and procedures as necessary to implement the privacy and civil liberties safeguards identified in E.O. 14086, and release the updated policies and procedures publicly to the maximum extent possible.

The Drug Enforcement Administration (DEA), Office of National Security Intelligence (ONSI), is an office within the DEA. Pursuant to Section 3 of the National Security Act of 1947, as amended, and Section 3.5(h) of E.O. 12333, as amended, ONSI is an element of the IC.

Pursuant to Section 1.7(i) of E.O. 12333, as amended, ONSI is only authorized to "[c]ollect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions."

ONSI is not authorized to conduct – and does not conduct – SIGINT activities.<sup>1</sup> Accordingly, ONSI does not engage in SIGINT collection or have access to unevaluated, raw, or unminimized SIGINT.

---

<sup>1</sup> References to SIGINT and SIGINT activities in this document also apply to Section 702 information.

### 3.0 POLICY AND PROCEDURES

The following applies to ONSI's safeguarding of personal information of non-U.S. persons collected through SIGINT activities, should ONSI knowingly come into possession of such information, and fulfill the principles contained in subsections 2.(a)(ii)-(iii) of E.O. 14086.<sup>2</sup> These procedures apply to individuals who operate under ONSI's EO 12333 authorities. Nothing in these procedures shall prohibit or regulate DEA's activities pursuant to its statutory criminal law enforcement and civil regulatory missions. This includes DEA's responsibilities pertaining to law enforcement information related to the domestic or foreign activities of U.S. persons.

#### A. Minimization

ONSI does not have access to unevaluated, raw, or unminimized SIGINT, including SIGINT collected in bulk. ONSI does receive finished intelligence products from other agencies that may include SIGINT information<sup>3</sup> that has been evaluated, and minimized subject to – among other requirements – the provisions of E.O. 14086.

##### 1. Dissemination

- a. Should ONSI knowingly handle SIGINT information, it will disseminate personal information of non-U.S. persons collected through SIGINT activities only if dissemination of comparable information concerning U.S. persons would be permitted under Section 2.3 of E.O. 12333.
- b. ONSI will disseminate personal information concerning a non-U.S. person on the basis that it is foreign intelligence only if the information relates to an authorized intelligence requirement, not solely because of the person's foreign nationality or country of residence. Unless it possesses specific information to the contrary, ONSI will presume that any evaluated or minimized information it receives from other IC elements that have adopted procedures implementing E.O. 14086 meets this standard. ONSI will disseminate such information in accordance with applicable DEA and IC policies and procedures, consistent with Section 2 (c)(iii)(A)(1) of E.O. 14086.
- c. ONSI shall disseminate within the U.S. Government such personal information 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.
- d. ONSI 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 SIGINT to

---

<sup>2</sup> These procedures do not alter the rules applicable to U.S. persons found in the Foreign Intelligence Surveillance Act, Executive Order 12333, ONSI's guidelines, or other applicable law.

<sup>3</sup> The sources or methods of obtaining specific information contained in evaluated or finished intelligence products may not in all cases be evident to ONSI as a recipient of such intelligence products.

recipients outside the U.S. Government, including to a foreign government or international organization.

- e. ONSI shall disseminate personal information collected through SIGINT only in accordance with, and never to circumvent these procedures.
- f. For purposes of these policies and procedures, "dissemination" shall mean the transmission, communication, sharing, or passing of information outside of ONSI by any means, including oral, electronic, or physical.

## 2. Retention

- a. Should ONSI knowingly handle SIGINT information, it will retain personal information of non-U.S. persons collected through SIGINT activities only if retention of comparable information concerning U.S. persons would be permitted under Section 2.3 of E.O. 12333, shall subject such information to the same retention periods that would apply to comparable information concerning U.S. persons, and shall delete such information that may no longer be retained in the same manner that comparable information concerning U.S. persons would be deleted.
- b. ONSI will retain personal information concerning a non-U.S. person on the basis that it is foreign intelligence in accordance with applicable DEA and IC policies and procedures, consistent with Section 2(c)(iii)(A)(2) of E.O. 14086 only if the information relates to an authorized intelligence requirement and not solely because of the person's foreign nationality or country of residence.
- c. Unless it possesses specific information to the contrary, ONSI will presume that any evaluated or minimized SIGINT information it receives from other IC elements that have adopted procedures implementing E.O. 14086 meets this standard. ONSI will retain such information in accordance with applicable record retention policies.

## B. Data Security and Access

- 1. Access to all personal information collected through SIGINT activities – irrespective of the nationality of the person whose information is collected – is restricted to those personnel who have a need to access that information in the performance of authorized duties in support of ONSI missions and have received appropriate training. Such information will be maintained in either electronic or physical form in secure facilities protected by physical and technological safeguards, including, but not limited to, adherence to certifications requirements and established standards, and with access limited by appropriate security measures. Such information will be safeguarded in accordance with applicable laws, rules and policies, including those in ONSI, DEA, and the IC, and through consultation with the Office of Chief Counsel (CC), as appropriate.
- 2. Classified information will be stored appropriately in a secured, certified, and accredited facility, in secured databases or containers, and in accordance with other applicable requirements. ONSI's electronic system in which such information may be stored will comply with applicable law, E.O.s, as well as IC

and DEA policies and procedures regarding information security, including access controls and monitoring.

#### C. Data Quality

ONSI does not produce intelligence products containing SIGINT; however, should it do so in the future, the personal information of both U.S. and non-U.S. persons collected through SIGINT activities – when identifiable – shall be included in ONSI intelligence products only as consistent with applicable IC standards of analytic tradecraft, accuracy, and objectivity as set forth in relevant IC directives, including Intelligence Community Directive 203: *Analytic Standards*. Particular care should be taken to apply standards relating to the relevance, quality, and reliability of the information, consideration of alternative sources of information and interpretations of data, and objectivity in performing analysis.

#### D. Oversight

1. As applicable, the Assistant Administrator for Intelligence/Chief of Intelligence (NC), or their designee, shall review implementation of these policies and procedures annually, focusing particularly on relevant provisions of E.O. 14086 regarding privacy and civil liberties.
2. Instances of non-compliance with these policies and procedures shall be reported to the Deputy Chief of Intelligence (NN) for ONSI, who shall report them to NC. The NC, in consultation with CC, as appropriate, shall determine what corrective actions are necessary, including, but not limited to, reporting to the appropriate DEA and IC oversight and compliance officials.
3. Should the NN determine that an instance of non-compliance constitutes a significant instance of non-compliance with applicable U.S. law the NN shall report it promptly to the NC, who shall notify the DEA Administrator and the Director of National Intelligence, consistent with Section 2(d)(iii) of E.O. 14086. A significant incident of non-compliance shall be determined consistent with Section 4(l) of E.O. 14086 after consultation with CC, as appropriate.

#### E. Redress Mechanism

1. ONSI shall provide the Office of the Director of National Intelligence (ODNI) Civil Liberties Protection Officer (CLPO) and the Privacy and Civil Liberties Oversight Board with access to information necessary to conduct the reviews described in either Section 3(c)(i), Section 3(d)(i), or Section 3(e)(i) of E.O. 14086, consistent with the protection of intelligence sources and methods.
2. ONSI personnel shall not take any actions designed to impede or improperly influence the CLPO's review of qualifying complaints or the Data Protection Review Court (DPRC) review of the CLPO's determination of such pursuant to the Signals Intelligence Redress Mechanism.
3. ONSI shall comply with any CLPO determination to undertake appropriate remediation, subject to any contrary determination of the DPRC, and, further, shall

comply with any determination by a DPRC panel to undertake appropriate remediation.

#### 4.0 TRAINING

ONSI personnel whose duties require access to personal information collected through SIGINT activities will receive annual training on the requirements of these policies and procedures pursuant to Section 3.0 paragraph D.1. of this policy and procedure. ONSI will monitor completion of training requirements to ensure compliance with this provision.

#### 5.0 DEVIATIONS FROM THESE PROCEDURES

The Principal Deputy Administrator must approve in advance any departures from these procedures after consultation with the ODNI and the National Security Division (NSD) of the Department of Justice (DOJ).

If there is insufficient time to obtain approval and a departure from these procedures is necessary because of the immediacy or gravity of a threat to the safety of persons, property, or national security, the NC, or designee, may approve a departure from these procedures. In this event, consultation shall occur with the Chief of the Intelligence Law Section, CC, and NC. NC, or their designee, will provide prompt written notice to the ODNI and the NSD, DOJ of any such departures, stating why advance approval was not possible and describing the actions taken to ensure activities were conducted lawfully. Notwithstanding this paragraph, all activities of ONSI must always be carried out in a manner consistent with the Constitution and laws of the United States, and E.O. 12333 and 14086.

#### 6.0 CONCLUSION

These procedures are set forth solely for internal guidance within ONSI in the event ONSI knowingly handles SIGINT in the future. Questions on the applicability or interpretation of these procedures should be directed to the CC, who shall determine such applicability or interpretation, in consultation with the Assistant Attorney General for National Security and the ODNI, as appropriate.

#### 7.0 EFFECTIVE DATE/REVISION HISTORY

*Table 1 Summary of Changes*

<b>Date of Change</b>	<b>Responsible Party</b>	<b>Summary of Change</b>
3/1/2023	Office of National Security Intelligence	Initial Publication
6/30/2023	Office of National Security Intelligence	The Office of the Director of Intelligence, the Privacy and Civil Liberties Oversight Board, and Department of Justice, National

Date of Change	Responsible Party	Summary of Change
		Security Division reviewed the above referenced Office of National Security Intelligence policy, and required several revisions to provide further clarification and consistency between the policies of the other Intelligence Community elements as much as possible given the different authorities among the elements.

**8.0 ACRONYMS**

*Table 2 Acronyms*

Acronym	Defined
CC	Office of Chief Counsel
CLPO	Civil Liberties Protection Officer
DEA	Drug Enforcement Administration
DOJ	Department of Justice
DPRC	Data Protection Review Court
E.O.	Executive Order
IC	Intelligence Community
ICD	Intelligence Community Directive
NC	Assistant Administrator for Intelligence/Chief of Intelligence
NN	Deputy Chief of Intelligence
NSD	National Security Division
ODNI	Director of National Intelligence
ONSI	Office of National Security Intelligence*
PPD	Presidential Policy Directive
SIGINT	Signals Intelligence

\* Outside of DEA, the Office of National Security Intelligence is referred to as ONSI in place of NN.