POLICY

OFFICE OF INTELLIGENCE AND ANALYSIS

OIA Policy Number	OIA-POL-04-003
Title	Safeguarding Personal Information Collected Through Signals Intelligence
Effective Date	June 30, 2023
Approved By	Shannon R. Corless Assistant Secretary

1) Background

Executive Order 14086, *Enhancing Safeguards for Signals Intelligence Activities* (October 7, 2022) (hereafter "E.O. 14086"), establishes safeguards for the handling of personal information collected through signals intelligence. E.O. 14086 requires, among other things, the head of each Intelligence Community (IC) element, within one year of the date of the Order, in consultation with the Attorney General, the Civil Liberties Protection Officer (CLPO) of the Office of the Director of National Intelligence (ODNI), and the Privacy and Civil Liberties Oversight Board (PCLOB), to update the element's policies and procedures issued pursuant to Presidential Policy Directive 28 of January 17, 2014, *Signal Intelligence Activities* (PPD-28), as necessary to implement the privacy and civil liberties safeguards in the E.O. 14086.

This document constitutes the updated policies and procedures used by the Department of the Treasury's Office of Intelligence and Analysis (OIA) for safeguarding personal information collected through signals intelligence, as required by E.O. 14086. These updated policies and procedures supersede OIA's policies and procedures issued under PPD-28, *PPD-28 Procedures for the Office of Intelligence and Analysis*, January 16, 2015.

OIA conducts its mission in accordance with the Constitution and with applicable statutes and Executive orders, proclamations, and other Presidential directives. Pursuant to section 1.7(i) of Executive Order 12333 of December 4, 1981, as amended, *United States Intelligence Activities*, OIA is authorized to collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions. OIA is not authorized to

conduct, and does not conduct, signals intelligence collection activities, nor does OIA have access to or conduct queries of unminimized signals intelligence acquired by other IC elements through bulk collection. OIA does, however, handle personal information collected through signals intelligence[1] by other IC elements and disseminated to OIA.

2) Scope

These policies and procedures shall be used by all OIA employees and contractors, employees of other agencies or departments who are detailed to OIA and perform OIA work under the direction and supervision of OIA, and any other Treasury components or employees when they are performing intelligence activities authorized pursuant to E.O. 12333 (collectively referred to as "OIA personnel").

3) Policies and Procedures

OIA does not conduct signals intelligence collection activities or bulk collection of signals intelligence. OIA does, however, receive disseminated signals intelligence information—including personal information—collected by other IC elements that has been evaluated, minimized, or otherwise included in finished intelligence products[2] subject to—among other requirements—the provisions of E.O. 14086.

OIA will apply the following policies and procedures for safeguarding personal information collected through signals intelligence. These policies and procedures shall fulfill the principles contained in subsections 2(a)(ii) and 2(a)(iii) of E.O. 14086.

A. Minimization

i. Dissemination

a. OIA shall disseminate non-United States persons' personal information collected through signals intelligence only if it involves one or more of the comparable

[1] References to signals intelligence and signals intelligence activities in this document also apply to intelligence collected and activities conducted pursuant to Section 702 of the Foreign Intelligence Surveillance Act.
[2] The sources of, or methods of, obtaining specific information contained in evaluated or finished intelligence products may not in all cases be evident to OIA or to the Treasury Department as a recipient of such intelligence products.

types of information that Section 2.3 of Executive Order 12333 states may be disseminated in the case of information concerning United States persons.

b. OIA shall disseminate personal information concerning a non-U.S. person collected through signals intelligence on the basis that it is foreign intelligence only if the information relates to an authorized intelligence requirement and not solely because of a person's nationality or country of residence.

c. OIA 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.

d. OIA 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.

e. OIA shall not disseminate personal information collected through signals intelligence for the purpose of circumventing the provisions of E.O. 14086.

ii. Retention

a. OIA shall retain personal information concerning a non-United States person collected through signals intelligence on the basis that it is foreign intelligence only if the information relates to an authorized intelligence requirement and the retention of comparable information concerning United States persons would be permitted under applicable law. OIA shall subject such information to the same retention periods that would apply to comparable information concerning a United States person.

b. OIA 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.

B. Data Security and Access

i. OIA 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, IC directives, and associated policies.

ii. OIA shall limit access to personal information collected through signals intelligence to authorized 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 these policies and procedures. OIA personnel will be considered to have met the training requirements in these policies and procedures if they are up to date in completing their required annual training on E.O. 12333, their required annual sensitive compartmented information training, and the annual training required by subsection E below.

iii. OIA's Chief Information Officer and Chief Information Security Officer, in consultation with the OIA Civil Liberties and Privacy Protection Officer (OIA CLPPO) and Treasury's Office of General Counsel (OGC), will ensure that the National Security Systems in which signals intelligence information is stored are certified under and adhere to established standards.

C. Data Quality

OIA shall include personal information collected through signals intelligence in intelligence products only as consistent with applicable IC standards for accuracy and objectivity—including Intelligence Community Directive 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 the data, and objectivity in performing analysis.

D. Deviations and Documentation

OIA's Assistant Secretary and the Assistant Attorney General for National Security, after consultation with OGC and ODNI, must approve in advance any departures from these policies and procedures. If there is not time for such an 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, OIA's Assistant Secretary may approve a departure from these procedures. OGC will be

notified as soon as possible. OIA's Assistant Secretary 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 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. Redress Assistance

OIA shall provide the ODNI CLPO with access to information necessary to conduct the reviews described in either Section 3(c)(i) or Section 3(d)(i) of E.O. 14086, consistent with the protection of intelligence sources and methods. OIA personnel shall not take any action designed to impede or improperly influence the ODNI CLPO's review of qualifying complaints or the Data Protection Review Court's (DPRC) review of the ODNI CLPO's determination of such pursuant to the Signals Intelligence Redress Mechanism. OIA shall comply with any ODNI 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.

OIA shall provide the PCLOB with access to information necessary to conduct the annual review of the redress process described in Section 3(e) of E.O. 14086, consistent with the protection of intelligence sources and methods.

F. Oversight

i. *Training.* OIA personnel who access information collected through signals intelligence must receive annual training on the requirements of E.O. 14086, these policies and procedures, and the policies and procedures for reporting and remediating incidents of non-compliance with applicable United States law. OIA will monitor completion of training requirments to ensure compliance with this provision.

ii. Incidents of non-compliance.

a. All OIA personnel should report potential instances of non-compliance with these policies and procedures to the OIA CLPPO. The OIA CLPPO, in coordination with OGC, shall promptly report instances of non-compliance to relevant entities to ensure their remediation, consistent with existing reporting

requirements under applicable law, regulation, Presidential direction, and policy. Should the OIA CLPPO, in coordination with OGC, determine that an incident of non-compliance is a "significant incident of non-compliance" as defined in Section 4(1) of E.O. 14086, the OIA CLPPO shall promptly report it to OIA's Assistant Secretary, the Secretary of the Treasury, and the Director of National Intelligence, who shall ensure that any necessary actions are taken to remediate it and prevent its recurrence and shall further ensure that any other relevant officials are notified, as appropriate.

b. Consistent with Treasury Department and IC policy and directives, all OIA personnel are required to report criminal activity, including fraud, waste, and abuse involving OIA or IC activities, operations, programs, or personnel to Treasury's Office of Inspector General (OIG) and/or to the Office of the Inspector General of the Intelligence Community (IC IG). OIA personnel also may report other potential instances of non-compliance with U.S. law, these policies and procedures, or other matters of concern to Treasury's OIG and/or the IC IG.

4) Roles and Responsibilities

A. OIA's Assistant Secretary

OIA's Assistant Secretary is responsible for issuing these policies and procedures and, as necessary, any updates or amendments hereto; issuing appropriate guidance to OIA personnel on the proper application of these policies and procedures; receiving reports of significant incidents of non-compliance with applicable United States law; and ensuring that any necessary actions are taken to remediate and prevent the recurrence of a significant incident of non-compliance with applicable United States law.

B. OIA's Civil Liberties and Privacy Protection Officer

OIA's Civil Liberties and Privacy Protection Officer (OIA CLPPO) is responsible for developing and maintaining appropriate training requirements to ensure that all OIA employees with access to signals intelligence know and understand the requirements of E.O. 14086 and these policies and procedures; and for conducting oversight of and ensuring compliance with applicable United States law. In addition, if the OIA CLPPO identifies or receives a report of a significant incident of non-compliance with applicable

United States law, the OIA CLPPO will report the incident promptly to OIA's Assistant Secretary, the Secretary of the Treasury, and the Director of National Intelligence.

C. Treasury's Office of General Counsel

Treasury's Office of General Counsel (OGC) is responsible for advising OIA's Assistant Secretary, OIA's CLPPO, and, as needed, other OIA personnel on the interpretation and implementation of the requirements of E.O. 14086 and these policies and procedures, and on the requirements of applicable United States law. In addition, if OGC identifies or receives a report of a significant incident of non-compliance with applicable United States law, it will report the incident promptly to OIA's Assistant Secretary, who in turn shall report the incident to the Secretary of the Treasury and the Director of National Intelligence.

D. All OIA Personnel

All OIA personnel are responsible for being familiar with, and for complying with, the requirements of E.O. 14086 and these policies and procedures. OIA personnel shall refer any questions concerning the interpretation or application of these policies and procedures to OIA's CLPPO and Treasury OGC. In addition, any OIA personnel who identifies a significant incident of non-compliance with applicable United States law is responsible for reporting the incident promptly to the OIA CLPPO or Treasury OGC.

5) Related Procedures and Guidance

Not used.

6) Authorities and References

31 U.S.C. §§ 311 and 312.

Executive Order 14086, *Enhancing Safeguards for United States Signals Intelligence Activities* (October 7, 2022).

Executive Order 12333, as amended, *United States Intelligence Activities*, (December 4, 1981).

PPD-28 Procedures for the Office of Intelligence and Analysis, January 16, 2015, hereby rescinded.

7) Definitions

Intelligence Community and **elements of the Intelligence Community**	"Intelligence Community" and "elements of the Intelligence Community" have the same meanings as they have in Executive Order 12333, as amended.
Dissemination	"Dissemination" means the transmission, communication, sharing, or passing of information outside OIA by any means, including oral, electronic, or physical means. It therefore includes providing any access to information in OIA's custody to a person outside OIA.
Non-United States person	"Non-United States person" means a person who is not a United States person.
Significant incident of non-compliance	"Significant incident of non-compliance" means a systemic or intentional failure to comply with a principle, policy, or procedure of applicable United States law that could impugn the reputation or integrity of an element of the Intelligence Community or otherwise call into question the propriety of an Intelligence Community activity, including in light of any significant impact on the privacy and civil liberties interests of the person or persons concerned.
United States person	"United States person" means a United States citizen, an alien know by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially comprised of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

8) Approval

OIA Leadership Approval	
Approver	**Shannon R. Corless**
Office, Title	**Assistant Secretary for Intelligence and Analysis**
Date	June 29, 2023
Signature	Shannon H. Corless Digitally signed by Shannon H. Corless Date: 2023.06.29 10:06:05 -04'00'