

Implementation Procedures for the Signals Intelligence Redress Mechanism Under Executive Order 14086

A. AUTHORITY: The National Security Act of 1947, as amended; Foreign Intelligence Surveillance Act of 1978, as amended; Executive Order (EO) 12333, as amended; Executive Order 13526, as amended; Executive Order 14086; Intelligence Community Directive (ICD) 107, Civil Liberties, Privacy, and Transparency; and other applicable provisions of law.

B. PURPOSE:

1. This Directive establishes the process for the submission of qualifying complaints transmitted by an appropriate public authority in a qualifying state pursuant to Executive Order 14086. Additionally, and pursuant to the same Executive Order, this Directive authorizes and sets forth the process through which the ODNI Civil Liberties Protection Officer (CLPO) shall investigate, review, and, as necessary, order appropriate remediation for a covered violation regarding qualifying complaints; communicate the conclusion of such investigation to the complainant through the appropriate public authority in a qualifying state and in a manner that protects classified or otherwise privileged or protected information; and provide necessary support to the U.S. Data Protection Review Court.

C. APPLICABILITY

1. This Directive applies to the Intelligence Community (IC), as defined by Executive Orders 12333 and 14086.

2. Nothing in this Directive is intended to alter or supersede ODNI's obligations or authorities under other applicable U.S. laws, regulations, or policy direction, to include, but not limited to: Executive Order 12333, Executive Order 14086, the Freedom of Information Act, the Privacy Act of 1974, the Foreign Intelligence Surveillance Act of 1978, or the Inspector General Act.

D. DEFINITIONS

1. The terms "appropriate remediation," "covered violation," "Intelligence Community," "elements of the Intelligence Community," "intelligence," "national security," and "qualifying complaint" shall have the same meaning as defined in Executive Order 14086.



2. A “qualifying state” is defined as a country or regional economic integration organization that has been designated by the Attorney General after a determination that the country or regional economic integration organization meets the requirements of Section 3(f) of Executive Order 14086.

3. An “appropriate public authority in a qualifying state” is defined as an entity that has been officially selected by the qualifying state to facilitate the consideration of qualifying complaints made with respect to data transfers from the qualifying state to the United States. A country or regional economic integration organization may identify its appropriate public authority in the course of seeking the Attorney General’s designation as a qualifying state pursuant to Section 3(f) of Executive Order 14086. A qualifying state may change or update its appropriate public authority at any time, with 30 days’ notice, through an official statement provided by its foreign ministry to the CLPO and the Department of State.

4. The “protection of intelligence sources and methods” is defined for the purpose of this Directive to include, but is not limited to, the protection of any classified information or otherwise privileged or protected information. These protections are to be applied in a manner that maintains the full and appropriate protection of all classified, privileged, or protected information, while still ensuring that the CLPO, Data Protection Review Court, and Privacy and Civil Liberties Oversight Board are provided access to information necessary to conduct the functions assigned to each of these entities by Executive Order 14086.

E. POLICY

1. Submission and Receipt of Qualifying Complaints:

a. Pursuant to Executive Order 14086, a complainant must submit a complaint in writing to the appropriate public authority in a qualifying state.

b. An appropriate public authority in a qualifying state must transmit the written complaint to the CLPO through an encrypted electronic communication. ODNI’s Office of Civil Liberties, Privacy and Transparency will establish an electronic address to receive such transmitted complaints from appropriate public authorities in qualifying states.

c. Within 15 business days of receipt of the complaint from the appropriate public authority in a qualifying state, the CLPO shall conduct an initial review of the complaint to assess whether the complaint meets all of the requirements necessary to conduct a redress review pursuant to Executive Order 14086 and this Directive (i.e., whether the complaint is a “qualifying complaint,” as that term is defined in EO 14086). Specifically, for a transmitted complaint to be a “qualifying complaint” consistent with Executive Order 14086’s definition of “covered violation” and “qualifying complaint,” the complaint must:

(1) allege a violation has occurred and arises from U.S. signals intelligence activities conducted after 7 October 2022 regarding data reasonably believed to have been transferred to the United States from a qualifying state after the effective date of the Attorney General’s designation for such a state;

(2) allege the violation regards such transferred data that pertains to personal information of or about the complainant, a natural person;

(3) allege that the violation adversely affects the complainant's individual privacy and civil liberties interests;

(4) allege that the violation also violates one or more of the applicable laws, orders, statutes, or procedures detailed in Section 4(d)(iii) of Executive Order 14086;

(5) include basic information to enable a review of the complaint, to include:

(a) information that forms the basis for alleging that a covered violation has occurred, which need not demonstrate that the complainant's data has in fact been subject to United States signals intelligence activities;

(b) the nature of the relief sought;

(c) the specific means (e.g., the complainant's email address or phone number) by which personal information of or about the complainant was believed to have been transmitted to the United States;

(d) the identities of the United States Government entities believed to be involved in the alleged violation (if known); and

(e) any other measures the complainant pursued to obtain the relief requested and the responses received through those other measures;

(6) not be frivolous, vexatious, or made in bad faith;

(7) be brought on behalf of the complainant, acting on that person's own behalf, and not as a representative of a governmental, nongovernmental, or intergovernmental organization; and

(8) contain a verification by the appropriate public authority in a qualifying state:

(a) of the identity of the complainant, and

(b) that the complaint satisfies the conditions of Section E.1.c.(1) – (7) of this Directive.

d. The complaint must be transmitted to the CLPO by the appropriate public authority in a qualifying state in the English language. The appropriate public authority in a qualifying state may translate the complaint on behalf of the complainant.

e. The transmission of the complaint from an appropriate public authority in a qualifying state must also contain a description of the manner in which the authority verified the identity of the complainant. The CLPO shall rely on the verification of the identity of the complainant by the appropriate public authority in a qualifying state, but should either the information provided by the appropriate public authority in a qualifying state or subsequent investigation of the complaint call into question the identity of the complainant, the CLPO may request additional information from the public authority in a qualifying state in a manner that does not reveal intelligence sources or methods or otherwise indicate whether an individual has, in fact, been the subject of signals intelligence activities.

f. If the CLPO determines that the complaint is not a qualifying complaint because it does not meet the conditions of Section E.1.c., or does not meet the conditions of Section E.1.d., of this Directive, the CLPO will provide written notification via encrypted electronic communication and in the English language to the appropriate public authority in a qualifying state of the deficiencies in the complaint.

g. If the CLPO determines that the complaint meets the conditions of Sections E.1.c. and E.1.d. of this Directive, the CLPO will provide written notification via encrypted electronic communication and in the English language to the appropriate public authority in a qualifying state that a qualifying complaint has been submitted and that an investigation will commence.

h. The CLPO shall maintain records in a secure and classified electronic repository of all submitted complaints, all communications regarding submitted complaints with the appropriate public authorities in qualifying states, and all determinations of whether transmitted complaints were determined to be qualifying complaints. Such records shall be maintained consistent with National Archives and Records Administration records control schedules.

i. Within 10 business days of notifying an appropriate public authority in a qualifying state that a complaint has been determined by the CLPO to meet the requirements of Section E.1.c. and E.1.d. of this Directive, the CLPO shall transmit via encrypted electronic communication to the Department of Commerce and the Data Protection Review Court an unclassified record regarding each qualifying complaint that provides only the identity of the complainant, the appropriate public authority in a qualifying state that transmitted the qualifying complaint, and the date when the qualifying complaint was transmitted to the CLPO.

2. Investigation of a Qualifying Complaint:

a. The CLPO shall exercise statutory and delegated authority to investigate each qualifying complaint.

b. In light of the allegations made in the complaint, the CLPO will request that the Privacy and Civil Liberties Officers of the relevant IC elements obtain and provide the CLPO access to information necessary to investigate the qualifying complaint.

(1) In a manner consistent with the protection of classified information or otherwise privileged or protected information, the CLPO, with assistance from the Privacy and Civil Liberties Officers of the relevant IC elements, will conduct an investigation by gathering information necessary to complete the review, to include, where appropriate, a description of the search parameters used to identify such information and written confirmation when no such information is identified. All searches and transmission of results must be conducted in a timely manner in order to facilitate the investigation.

(2) The CLPO may: seek clarifications; request additional information or documents regarding the relevant signals intelligence activities or remedial steps taken in the case of previously identified noncompliance regarding relevant signals intelligence activities; conduct and document interviews with relevant IC personnel; or otherwise seek the assistance of the IC elements, through their Privacy and Civil Liberties Officers, in any instances in which the CLPO determines it is necessary to supplement the record in order to investigate the allegations of a

qualifying complaint. IC elements shall provide access to information and personnel in a manner consistent with the protection of classified information or otherwise privileged or protected information.

(3) The CLPO may also request information from the Department of Justice regarding any legal advice provided, or compliance records concerning, signals intelligence activities related to the allegations in the qualifying complaint.

c. IC elements shall not take any actions designed to impede or improperly influence the investigation of the CLPO into facts relevant to the qualifying complaint.

d. The information and records obtained by the CLPO shall be maintained in a physically or logically separated repository with protections necessary to protect classified or otherwise privileged or protected information and in a manner consistent with National Archives and Records Administration records control schedules.

3. Review, Determination, and Remediation of Qualifying Complaints:

a. Based upon the result of the investigation, the CLPO shall determine whether a covered violation has occurred. In making this determination, the CLPO shall apply relevant U.S. law impartially, and consistent with established legal principles, take into account both relevant national security interests and applicable privacy protections, and give appropriate deference to any relevant determinations made by national security officials.

b. If the CLPO determines that a covered violation has occurred, the CLPO will determine the appropriate remediation for the covered violation.

c. As required by Executive Order 14086, each element of the IC, and each agency containing an element of the IC, shall comply with any applicable determination by the CLPO to undertake appropriate remediation with regard to the qualifying complaint, subject to any contrary determination by the Data Protection Review Court. Information regarding the status and completion of such appropriate remediation shall be provided to the CLPO.

d. The CLPO shall produce a classified written decision explaining the basis for the CLPO's factual findings, determination with respect to whether a covered violation occurred, and determination of the appropriate remediation in the event of a covered violation. The CLPO's classified written decision, as well as any relevant information or records obtained or created by the CLPO in the course of the investigation, shall constitute the classified ex parte record of review. The classified ex parte record of review shall be maintained in a physically or logically separated repository with protections necessary to protect classified or otherwise privileged or protected information, in a manner consistent with National Archives and Records Administration records control schedules.

e. The CLPO shall provide a classified report on information indicating a violation of any authority subject to the oversight of the Foreign Intelligence Surveillance Court to the Assistant Attorney General for National Security to permit onward reporting to the Court, as required by law or the Court's Rules of Procedure.

4. Transmittal of Results of Review of Qualifying Complaint:

a. Upon the CLPO's completion of the review of a qualifying complaint, and in a manner that continues to protect classified information or otherwise privileged or protected information, the CLPO shall provide a copy of the CLPO's classified written decision to all relevant IC elements. IC elements may seek review of the CLPO's classified decision by the Data Protection Review Court in the manner prescribed by Executive Order 14086 and regulations issued by the Attorney General.

b. Upon the CLPO's completion of the review of a qualifying complaint, the CLPO shall inform the complainant, in writing and via an unclassified statement in the English language and made via an encrypted electronic communication to the appropriate public authority in a qualifying state, in a manner that continues to protect classified information or otherwise privileged or protected information, and without confirming or denying that the complainant was subject to United States signals intelligence activities, that:

(1) The review either did not identify any covered violations or the Civil Liberties Protection Officer of the Office of the Director of National Intelligence issued a determination requiring appropriate remediation;

(2) The complainant or an element of the IC may, as prescribed in regulations issued by the Attorney General, apply for review of the CLPO's determinations by the Data Protection Review Court described in Executive Order 14086, to include a statement on the manner in which the complainant may seek review from the Data Protection Review Court pursuant to these regulations; and

(3) If either the complainant or an element of the IC applies for review by the Data Protection Review Court, a special advocate will be selected by the Data Protection Review Court to advocate regarding the complainant's interest in the matter.

5. Assistance to the Data Protection Review Court:

a. In the event that a Data Protection Review Court panel is convened, the CLPO shall convey to the Data Protection Review Court the classified ex parte record of review in a manner consistent with the relevant regulations approved by the Attorney General and requirements governing the handling of classified information or otherwise privileged or protected information.

b. The CLPO shall provide any necessary support as requested by the Data Protection Review Court, to include supplementing the classified ex parte record of review in response to inquiries made by the Data Protection Review Court.

c. Consistent with statutory and delegated authority, and in a manner consistent with the protection of intelligence sources and methods, the CLPO will request from IC elements assistance in obtaining information to supplement the classified ex parte record of review in response to requests from the Data Protection Review Court.

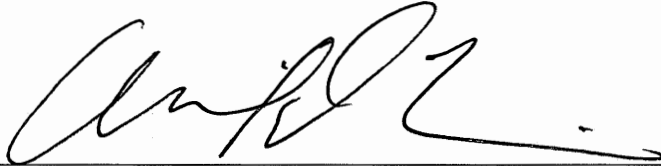
d. Consistent with the relevant regulations issued by the Attorney General, should the Data Protection Review Court determine that alternative appropriate remediation is required to fully redress the qualifying complaint, the CLPO shall consult with relevant IC elements and provide views to the Data Protection Review Court regarding the alternative appropriate

remediation, to include an assessment of the impacts of such alternative appropriate remediation on the operations of the IC and the national security of the United States.

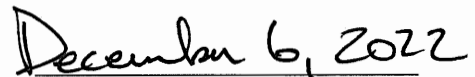
6. Assistance to the Privacy and Civil Liberties Oversight Board (PCLOB):

a. IC elements and the CLPO shall provide the PCLOB with access to information necessary to conduct the annual review of the redress process described in Section 3(e) of Executive Order 14086, consistent with the protection of intelligence sources and methods.

F. EFFECTIVE DATE: This Directive becomes effective on the date of signature.



Director of National Intelligence



Date