Executive Order 14086: Signals Intelligence Redress Mechanism

The Role of the ODNI CLPO

Frequently Asked Questions (FAQs) Table of Contents

ODNI and CLPO

What is the ODNI?

- The ODNI is the Office of the Director of National Intelligence.
- The Director of National Intelligence (DNI) leads the Intelligence Community (IC) and is the principal advisor to the President for intelligence matters related to national security.
- The DNI's authority and duties are set forth in statute, including principally in the National Security Act of 1947, as amended by the Intelligence Reform and Terrorism Prevention Act of 2004, and in Executive Order.
- For more information on the ODNI, please visit the ODNI website.

Who is the ODNI CLPO?

- The ODNI's Civil Liberties Protection Officer (CLPO) is a position created by the Intelligence Reform and Terrorism Prevention Act of 2004 and codified into Section 103D of the National Security Act of 1947 (50 U.S.C. § 3029).
- The ODNI CLPO reports directly to the DNI and is the Chief of ODNI's Office of Civil Liberties, Privacy, and Transparency (CLPT).
- Intelligence transparency is integral to the execution of CLPT's duties pursuant to § 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007. CLPT has developed or supported efforts across the IC to explain in a more clear, concise, and effective manner the mission, activities, authorities, privacy safeguards, and oversight mechanisms of the IC.
- The CLPO leads the integration of civil liberties and privacy protections into the policies and procedures of the ODNI and the IC.
- The CLPO further oversees ODNI's compliance with laws, regulations, Executive Orders, and implementing guidelines relating to civil liberties and privacy; and reviews and assesses complaints, among other specified duties.
- The CLPO is also the ODNI's Chief Transparency Officer, responsible for leading implementation of the *Principles of Intelligence Transparency* for the IC and providing appropriate transparency about the IC's activities and authorities.

For more information on the ODNI CLPO, please visit the ODNI CLPT website.

Executive Order (E.O.) 14086

What is an Executive Order?

- An Executive Order is a Presidential directive through which the President manages the operations of the executive branch. Executive Orders are binding on the executive branch and may further clarify existing laws.
- The U.S. IC is part of the executive branch and must comply with Executive Orders.

What is Executive Order (E.O.) 14086?

- E.O. 14086 strengthens the privacy and civil liberties safeguards governing U.S. signals intelligence activities and directs additional steps to implement commitments under the European Union (EU)-U.S. Data Privacy Framework (EU-U.S. DPF).
- President Biden signed E.O. 14086 on October 7, 2022.
- E.O. 14086, "*Enhancing Safeguards for United States Signals Intelligence Activities,*" applies to signals intelligence activities of the IC.
- It establishes enhanced privacy and civil liberties safeguards for U.S. signals intelligence activities, beyond those in existing U.S. law.
- It establishes a new process enabling individuals in qualifying states to seek redress if they believe their personal data was collected through U.S. signals intelligence activities in a manner that violated applicable U.S. law (referred as the redress mechanism).
- For additional information refer to the White House's October 7, 2022 Fact Sheet.

Does E.O. 14086 only apply to EU citizens?

- No, the redress mechanism established under E.O. 14086 Section 3 extends to any individual who reasonably believes that his or her data was transferred from a country or regional economic integration organization that has been designated as a qualifying state (such as the EU) to the United States.
- E.O. 14086 provides enhanced privacy safeguards for U.S. signals intelligence activities. It recognizes that all persons, regardless of their nationality or wherever they might reside, have legitimate privacy interests in the handling of their personal information.
- E.O. 14086 implements the U.S. commitments made under the EU-U.S. DPF and the United Kingdom Extension to the EU-U.S. DPF and provide organizations with reliable mechanisms to transfer personal data from those locations while ensuring that data is protected consistent with the laws in those locations.

For additional information about the EU-U.S. DPF and other frameworks, refer to the Department of Commerce's DPF Program website.

Redress Mechanism Under E.O. 14086

What is the redress mechanism created by E.O. 14086?

- E.O. 14086 created a new two-layer mechanism for individuals to obtain independent and binding review and redress of "qualifying complaints" that their personal information, collected through U.S. signals intelligence, was collected or handled by the U.S. Government in violation of applicable U.S. law. *See* E.O. 14086 §§ 3(a), 4(k).
- Under the first layer, the ODNI CLPO will investigate and review qualifying complaints to determine whether a covered violation occurred and, as necessary, will order the appropriate remediation. *See* E.O. 14086 § 3c.
- Under the second layer, a panel of the Data Protection Review Court (DPRC) provides independent and binding review of the CLPO's determination, upon receipt of an application for review from the individual or an element of the IC. *See* E.O. 14086 § 3(d).

What is the ODNI CLPO's role under the redress mechanism?

- E.O. 14086 builds on the existing statutory role, functions, and independence of the ODNI CLPO. The ODNI CLPO is responsible for overseeing compliance with legal and policy protections relating to civil liberties and privacy, investigating possible abuses of civil liberties and privacy in the administration of ODNI programs and operations, and leading the integration of civil liberties and privacy protections across the entire U.S. IC.
- Given its duty to integrate civil liberties and privacy protections across the U.S. IC, the ODNI CLPO collaborates with IC elements' respective privacy and civil liberties officers to advance this duty.
- Under E.O. 14086, the CLPO has statutory and delegated authority to investigate, review, and, as necessary, order appropriate remediation for qualifying complaints under the redress mechanism.
- For more information on the ODNI CLPO, please visit the ODNI CLPO website.

How is the ODNI CLPO independent in the redress mechanism?

- E.O. 14086 specifically directs that the DNI may not interfere with a review by the CLPO of a qualifying complaint; nor may the DNI remove the CLPO for actions taken pursuant to the E.O. *See* E.O. 14086 § 3(c)(iv).
- E.O. 14086 authorizes the ODNI CLPO to issue binding determinations concerning qualified complaints submitted under the new redress mechanism, subject to the DPRC's review. *See* E.O. 14086 § 3(c)(ii).
- E.O. 14086 specifically directs that each IC element must provide the CLPO with access to information necessary to conduct the CLPO's reviews of qualifying complaints and may not take any actions designed to impede or improperly influence the CLPO's reviews. *See* E.O. 14086 § 3(c)(iii).

The Appropriate Public Authority

Who is my public authority?

- E.O. 14086 directs that the appropriate public authority in a qualifying state must transmit qualifying complaints to the ODNI CLPO. *See* E.O. 14086 § 3(c)(iv).
- The IC Directive 126 (ICD 126), *"Implementation Procedures for the Signals Intelligence Redress Mechanism Under Executive Order 14086,"* establishes the processes for submitting a qualified complaints, including by the appropriate public authority. *See* ICD 126 § D.3.
- To date, the following countries or regional economic integration organizations have been designated as qualifying states and have selected the following appropriate public authorities to transmit qualifying complaints to the CLPO:

Qualifying State	Public Authority	Additional Information
The European Union (EU), Iceland, Liechtenstein, and Norway	European Data Protection Board (EDPB)	If you are located in the EU or the European Economic Area (EEA), you must submit a complaint to your national data protection authority for transmission. The national data protection authority will ensure that the complaint is provided to the EDPB, who will then transmit qualifying complaints to the CLPO. Please go to the EDPB website for additional direction.
United Kingdom (U.K.)	Information Commission Office (U.K. ICO)	If you are located in the U.K., you must submit your complaint to the U.K. ICO. The U.K. ICO will then transmit qualifying complaints to the CLPO. Please go to the U.K. ICO website for additional direction.

For more information regarding designations by the Attorney General, please visit the Department of Justice's Executive Order 14086 website.

Complaints

What is a qualifying complaint?

❑ The complaint is:

- ✓ Submitted in writing, and
- ✓ Transmitted by the appropriate public authority in a qualifying state after the public authority has verified (a) the complainant's identity and (b) that the complaint satisfies the criteria in Section 4(k).

❑ The complaint alleges that a covered violation:

- ✓ Occurred after 7 October 2022 (the date E. O. 14086 was signed) and
- ✓ Concerns data reasonably believed to have been transferred to the U.S. from the qualifying state after the effective date of the Attorney General's designation.

❑ The alleged violation is about an individual's personal data.

- ✓ Complaint is submitted by the individual or brought on behalf of the individual.
- ✓ Complaint is not submitted as a representative of a government, nongovernmental, or intergovernmental organization.

❑ The complaint alleges that the violation:

- ✓ Adversely affects complainant's individual privacy and civil liberties interests and
- ✓ Violates U.S. laws, orders, or procedures specified in E. O. 14086 Section 4(d)(iii).

❑ The complaint provides basic information to enable a review:

- ✓ The basis for the complaint and relief sought;
- ✓ The specific means (such as an email address or phone number) by which the data was believed to have been transferred to the U.S;
- ✓ U.S. Government entities believed to be involved (if known); and
- ✓ Other measures the complainant pursued to obtain relief and the responses.

KEY POINT

The complaint need not demonstrate that the individual's data was in fact subject to U.S. signals intelligence activities

❑ The complaint is in good faith and not frivolous or vexatious.

- ✓ ICD 126 Section E.1. provides additional information about the steps the CLPO will take when verifying that a submitted complaint is a qualifying complaint.

What is a covered violation?

E.O. 14086 Section 4(d) defines a "covered violation" as a violation that:

1) Arises from signals intelligence activities conducted after the date of the E.O. regarding data transferred to the U.S. from a qualifying state after the effective date of the Attorney General's designation for that state;

2) Adversely affects the complainant's individual privacy and civil liberties interests; *and*

3) Violates U.S. laws, orders, procedures, or policies that provide privacy and civil liberties safeguards with respect to U.S. signals intelligence activities within the scope of E.O. 14086 and as further specified in Section 4(d)(iii) of the E.O.

Who can submit a complaint?

- An individual, or someone on behalf of an individual.

Can an individual submit a complaint directly to the CLPO?

- No. All complaints must be submitted, in writing, to an appropriate public authority in a qualifying state. *See* E.O. 14086 § 4(k). Refer to the authorities' websites links provided above.
- The appropriate public authority will then verify and transmit the complaint to the CLPO. *See* E.O. 14086 § 4(k).

KEY POINT

Submit your complaint to your public authority.

Only your public authority may transmit complaints to the CLPO.

How do I know if my country has been designated as a qualifying state?

- The U.S. Attorney General makes these designations. Information may be found at: Office of Privacy and Civil Liberties | Executive Order 14086 (justice.gov)
- To date, the Attorney General designated the European Union, Iceland, Liechtenstein, Norway, and the United Kingdom as "qualifying states."

May I still submit a complaint if I believe my data has been transferred to the United States from a state that has not been designated as a "qualifying state"?

- No, only individuals who reasonably believe that their data was transferred from a qualifying state to the United States may submit a complaint under E.O. 14086's redress mechanism. *See* E.O. 14086 § 4(d)(i).

If the country in which I reside has not been designated a qualifying state, does that mean that none of the privacy protections in the rest of E.O. 14086 apply to me?

- No, the designation of qualifying states only applies to which individuals may submit, through an appropriate public authority, a complaint to the CLPO or a request for review by the DPRC.
- The other privacy safeguards established in E.O. 14086 apply regardless of your location or nationality or whether your country of residence has been designated a qualifying state.

When can a complaint be submitted?

- To be a qualifying complaint, a complaint must allege that a covered violation:
  - ✓ Arises from signals intelligence activities that occurred after October 7, 2022 (the date that E.O. 14086 was signed); *and*
  - ✓ Regards data reasonably believed to have been transmitted to the United States after a country or regional economic integration organization was designated as a qualifying state. *See* E.O. 14086 § 4(d)(i).

Do I have to prove my data was transferred after the qualifying state was designated?

- No, E.O. 14086 requires only that an individual complainant "reasonably believes" that his or her data was transferred after the country or regional economic integration organization was designated. *See* E.O. 14086 § 4(k)(i).
- Further, E.O. 14086 specifies that complaints "need not demonstrate that the complainant's data had in fact been subject to United States signals intelligence activities." *See* E.O. 14086 § 4(k)(ii) (emphasis added).

What information do I need to provide when submitting a complaint?

- Section 4(k)(ii) specifies that a qualifying complaint must include the following basic information to enable a review by the CLPO:
  - ✓ 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;
  - ✓ the nature of the relief sought;
  - ✓ the specific means by which personal information of or about the complainant was believed to have been transmitted to the U.S.;
  - ✓ the identities of the U.S. Government entities believed to be involved in the alleged violation (if known); *and*
  - ✓ any other measures the complainant pursued to obtain the relief requested and the response received through those other measures.

CLPO's Role

What does the CLPO do when it receives a complaint?

- The CLPO reviews the complaint to determine if it meets the criteria of a qualifying complaint. If it does, the CLPO follows the process specified in the E.O. to investigate and review qualifying complaints; determine if a covered violation occurred; and, if necessary, order appropriate remediation, among other steps required by the E.O.

ICD 126 Section E.1. provides that the CLPO must:

- Conduct an initial review of the complaint (within 15 business days of receiving a complaint from an appropriate public authority) to assess whether the complaint is qualifying.
- Provide written notification to the complainant through the appropriate public authority that the complaint is either (a) not qualifying due to the specified deficiencies or (b) qualifying and an investigation will commence.
- Maintain records of all submitted complaints appropriately.
- Submit an unclassified record of each qualifying complaint to the Department of Commerce and the DPRC within 10 business days.
- Investigate each qualifying complaint and request information from each relevant IC element, as well as the Department of Justice, as necessary, to investigate the complaint.
- Determine whether a covered violation has occurred and, if so, determine the appropriate remediation.
- Inform the complainant through the appropriate public authority that:
  1) the review either did not identify any covered violations or the CLPO issued a determination requiring appropriate remediation; and
  2) the complainant may apply for review of the CLPO's determinations by the DPRC.

What steps can the CLPO take to remedy a covered violation of law?

- E.O. 14086 Section 4(a) defines "appropriate remediation" as lawful measures designed to fully redress an identified covered violation regarding a specific complainant and complaint.
- Section 4(a) specifies that such appropriate remediation may include, but is not limited to:
  - ✓ Administrative measures to remedy procedural or technical violations relating to otherwise lawful access,
  - ✓ Terminating acquisition of data where collection is not lawfully authorized,
  - ✓ Deleting data acquired without lawful authorization,
  - ✓ Deleting results of inappropriate queries on lawfully collected data, and
  - ✓ Restricting access to lawfully collected data to those appropriately trained.
- Each IC element must comply with the CLPO's determination regarding appropriate remediation (*see* E.O. 14086 Section 3(c)(ii)), subject to any contrary determination by the DPRC.

Notification

Will I get notice that my complaint was accepted as qualified?

- The ODNI CLPO will provide notification within 15 business days of receipt of the complaint from the appropriate public authority *to the appropriate public authority* that the complaint was either qualified or not qualified.
- For information as to how and when the appropriate public authority will notify you, please contact your appropriate public authority (website links are provided in the section above).

How will I know if the CLPO found a violation of law in relation to my complaint and how will I know what remedies were ordered?

- E.O. 14086 Section 3(c)(i)(E)(1) requires the CLPO, after determining whether a covered violation alleged in a qualified complaint occurred, to inform the complainant through the appropriate public authority that: "the review either did not identify any covered violations or the [ODNI CLPO] issued a determination requiring appropriate remediation."

What actions may I take after the CLPO has made a determination?

- After the CLPO provides notification to the appropriate public authority, the complainant may apply for review of the CLPO's determinations to the DPRC. *See* E.O. 14086 § 3(c)(i)(E)(2). Refer to "Seeking Court Review" below.

Will classified information about my complaint be declassified?

- It depends. E.O. 14086 and other U.S. laws, require that properly classified information be protected.
- E.O. 14086 Section 3(d)(v) specifies that no later than 5 years after the date of the E.O. and no later than every five years thereafter, the Secretary of Commerce will contact the relevant IC elements to determine whether information regarding the review of any complaint by the CLPO has been declassified and whether information regarding the review of any application for review submitted to the DPRC has been declassified.
- If such information has been declassified, the Department of Commerce will notify the complainant, through the appropriate public authority in a qualifying state, that information pertaining to the review of their complaint by the CLPO or to the review of any application for review submitted to the DPRC may be available under applicable law.
- In addition, E.O. 13526, provides a system for classifying, safeguarding, and declassifying national security information and requires that information be declassified as soon as it no longer meets the standards for classification under that executive order. *See* E.O. 13526 §3.2.
- Further, the *Principles of Intelligence Transparency* for the IC were also created to facilitate IC decisions on making information publicly available in a manner that enhances public understanding of intelligence activities, while continuing to protect information when disclosure would harm national security.

Seeking Court Review

When can I seek review by the Data Protection Review Court (DPRC)?

- A complainant may seek DPRC review only after the ODNI CLPO has completed review of the qualifying complaint and notified the complainant through the appropriate public authority of the CLPO's determinations.
- If a complainant wants to seek review by the DPRC, he or she must transmit a request through the appropriate public authority; complainants may not submit their requests directly to the DPRC.
- For information on submitting a request for a DPRC review through your appropriate public authority, please refer to the section above that provides websites for appropriate public authorities.

Where can I find more information about the Data Protection Review Court and how to seek review?

- For more information about the Data Protection Review Court, please visit Office of Privacy and Civil Liberties | DPRC Resources (justice.gov).