

UNCLASSIFIED

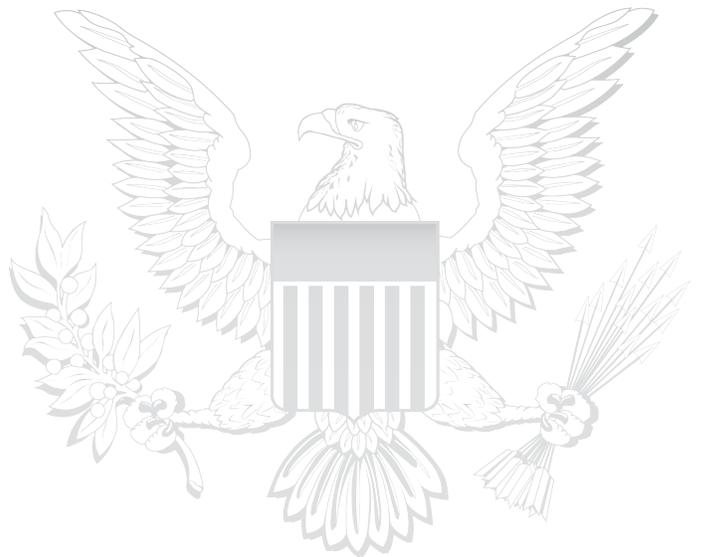


Office of the Director of National Intelligence

Office of Civil Liberties, Privacy, and Transparency Annual Report

(1 January 2024 to 31 December 2024)

November 2025



UNCLASSIFIED

Contents

Message from the Chief	2
About the Office of Civil Liberties, Privacy, and Transparency	4
Overview	6
Review, Advice, Assessment, Training, and Oversight Activities	7
Commercially Available Information	7
CNSS Privacy Overlays	7
CLPT’s Advice to ODNI, Review of ODNI Activities, and Related Training	8
NCTC	9
NCSC	9
Other ODNI Directorates, Components, and Offices.....	10
CLPT’s Advice to U.S. Government-Wide Efforts	10
Intelligence Oversight.....	11
E.O. 12333 Guidance and Oversight.....	11
FISA Joint Oversight	12
Intelligence Transparency, Engagement, and Outreach	13
International Privacy Forum	13
Transparency to External Overseers	16
The Intelligence Community Civil Liberties and Privacy Council and the Intelligence Transparency Council..	16
Complaints	16
Complaints Submitted Per E.O. 14086	18
Metrics	19
Complaints Relating to the Privacy Act and Privacy and Civil Liberties (Not Submitted Under E.O. 14086)	19
Complaints Submitted Under E.O. 14086	20
Conclusion	21
Appendix A: Acronyms/Abbreviations	22

Message from the Chief

As the Civil Liberties Protection Officer (CLPO) for the Office of the Director of National Intelligence (ODNI); the Chief of ODNI's Office of Civil Liberties, Privacy, and Transparency (CLPT); and ODNI's Chief Transparency Officer, I am pleased to present this report concerning CLPT activities from 1 January 2024 to 31 December 2024, as required by Section 1062 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004¹. This report provides an overview of the work ODNI's CLPT dedicated team of professionals accomplished during that time.



There were several major initiatives during the reporting period, including:

- *Commercially Available Information (CAI)*: In collaboration with the ODNI Open Source Executive, CLPT supported the implementation of the CAI Framework, which was published in May 2024. This framework provides guidance for the Intelligence Community (IC) access, collection, and processing of CAI, including specific rules related to sensitive CAI involving U.S. person information.
- *Committee on National Security Systems (CNSS)*: CLPT partnered with the National Security Agency's Civil Liberties, Privacy, and Transparency Office and co-led the interagency CNSS Privacy Sub-Working Group, which developed the CNSS Instruction No. 1253F Attachment 6, "Privacy Overlays." The Privacy Overlays were issued on 31 October 2024.
- *Executive Order (E.O.) 14086*: CLPT continued outreach on the redress mechanism to receive complaints under E.O. 14086 from individuals in qualifying states, including by publishing materials online and engaging with data protection regulators from the European Union (EU), Switzerland, and the United Kingdom. The ODNI CLPO received the first qualifying complaint under the redress mechanism. The ODNI CLPO supported the EU-U.S. Joint Review of the Data Privacy Framework (DPF) related to the implementation of the supplemental procedures.
- *1st Annual International Intelligence Privacy Forum*: CLPT hosted a collaborative forum for the Five Eyes (FVEY) and European intelligence services to gather and discuss privacy safeguards and transparency.

It is the mission of every intelligence agency throughout the world to provide decision advantage to its leaders. In the United States, IC elements accomplish this mission by complying with the law and respecting the foundational values of our free society. Top among these values is protecting privacy and civil liberties and incorporating an appropriate

¹ Pub. L. No. 108-458, 118 Stat. 3638 (2004).

level of transparency to engender and enhance public trust. It is the responsibility of every intelligence professional to act in accordance with these values.

I am proud that CLPT successfully continued to provide advice, conduct reviews, and handle complaints regarding privacy and civil liberties within ODNI, while continuing to integrate the privacy, civil liberties, and transparency efforts of the broader IC.

REBECCA J. RICHARDS

ODNI Civil Liberties Protection Officer;
ODNI Chief Transparency Officer; and
Chief of the Office of Civil Liberties, Privacy, and Transparency

About the Office of Civil Liberties, Privacy, and Transparency

CLPT collaborates closely with ODNI's directorates, components, and offices to understand in detail their initiatives and projects that may impact civil liberties or privacy, or benefit from increased transparency. ODNI initiatives and projects start with articulating the intelligence purpose for specific activities, the authority under which the activity is taken, and the characteristics and use of the data. CLPT reviews individual initiatives and projects to advise on civil liberties and privacy safeguards.

CLPT reviews policies, procedures, instructions, standards, guidance, databases, and systems containing personal information, testimony, proposed legislation, reports, releases, and other materials to ensure that privacy and civil liberties issues are appropriately addressed and properly articulated. CLPT also reviews the use of technology, especially new technologies, to ensure that such use enhances and does not erode privacy and civil liberties safeguards. These reviews may pertain specifically to ODNI or to other IC elements to the extent that the issues fall within ODNI's IC-wide responsibilities.

CLPT also oversees compliance with requirements under the Constitution and all laws, regulations, and procedures relating to privacy and civil liberties. Specifically, CLPT ensures that ODNI accesses, handles, and retains personal information in compliance with the Privacy Act. Furthermore, CLPT is responsible for oversight of ODNI's Attorney General Guidelines under E.O. 12333 and of ODNI's implementation procedures under E.O. 14086. Additionally, CLPT conducts joint oversight, along with other ODNI offices and the Department of Justice (DOJ), of the IC's implementation of Section 702 of the Foreign Intelligence Surveillance Act (FISA).

As it pertains to E.O. 14086, CLPT supports the ODNI CLPO in performing three key roles across the IC:

- First, Section 2(b)(iii) directs the CLPO to assess whether anticipated signals intelligence (SIGINT) collection activities conducted under the National Intelligence Priorities Framework (NIPF) (1) advance the defined legitimate objectives, (2) are neither designed nor anticipated to result in SIGINT collection in contravention of defined prohibited objectives, and (3) have been established after appropriate consideration of the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.
- Second, Section 2(c)(iv) requires the CLPO to be consulted when the IC elements update their procedures to comply with E.O. 14086, including making updates necessary to implement privacy and civil liberties safeguards.
- Third, Section 3(c) directs the CLPO to play a critical role in the multi-level, independent, and binding complaint mechanism that enables individuals in qualifying states to seek redress for a covered violation arising from U.S. SIGINT

activities related to their personal data that was reasonably believed to have been transferred from the qualifying state to the United States.

In addition to investigating qualifying complaints under E.O. 14086, the CLPO reviews and investigates, as appropriate, alleged abuses of privacy and civil liberties. When the CLPO receives a complaint, she must determine whether the complaint was directed to her office correctly or if it should have been referred to a different office or agency. For instance, depending on the circumstances, certain complaints may be referred to the IC Inspector General, the Office of Equal Employment Opportunity, or another agency. If the CLPO determines a complaint is not frivolous and merits a full review, she obtains and analyzes relevant information in accordance with pertinent legal and policy standards. Based on her findings, the CLPO determines the appropriate course of action to resolve the complaint and notifies the complainant of the disposition.

The CLPO also serves as ODNI's Chief Transparency Officer. CLPT is responsible for leading the implementation of the *Principles of Intelligence Transparency for the Intelligence Community*.² These principles guide how the IC makes information available to the public in a manner that enhances public understanding of intelligence activities, while still protecting information that, if disclosed, could harm national security.

Along with promoting transparency to the public, CLPT plays a key role in advancing transparency to oversight bodies. For example, it facilitates the submission of relevant compliance reports to the President's Intelligence Oversight Board (IOB), the Privacy and Civil Liberties Oversight Board (PCLOB), and the appropriate Congressional committees. Additionally, CLPT supports the provision of relevant materials and briefings to overseers regarding the IC's privacy and civil liberties safeguards.

CLPT further focuses transparency efforts inward to ensure that the IC workforce understands the privacy and civil liberties safeguards that all IC officers are required to follow. For example, CLPT leads privacy training for ODNI, including training focused on new employees and annual training for all employees. CLPT hosts the annual IC Civil Liberties, Privacy, and Transparency Summit to share information on safeguards, especially relating to current relevant topics across the IC. CLPT leads the IC Civil Liberties and Privacy Council (CLPC) and the Intelligence Transparency Council (ITC) to ensure that CLPOs and transparency officers within the IC have a frequently held forum to share new information and best practices.

CLPT carries out its duties in close consultation with other offices at ODNI and throughout the IC that have relevant and complementary responsibilities, including offices of

² Office of the Director of National Intelligence, *Principles of Intelligence Transparency for the Intelligence Community* (2015), <https://www.intelligence.gov/transparency>.

general counsel (OGC), offices of inspectors general, intelligence oversight offices, civil liberties and privacy offices, and the DOJ.

Overview

As part of its established mission, CLPT has continued its critical function of providing privacy and civil liberties advice, assessment, oversight, engagement, and transparency to the ODNI and IC elements. Additionally, CLPT has conducted extensive outreach, including speaking at conferences, engaging with non-governmental organizations (NGO), academics, and the press, and engaging with foreign partners and an international audience. CLPT has played key leadership roles in the U.S. Federal Privacy Council (FPC) and has also led the CLPC and the ITC. Furthermore, CLPT has continued to lead the interagency on interactions with the PCLOB and the IOB.

Table 1: 2024 CLPT Activities

2024 Review, Advice, Assessment, Training, and Oversight	Total
CLPT Review, Advice, and Assessments	40
Number of Education and Training Sessions conducted by CLPT ³	43
CLPT Oversight Reviews ⁴	18
Total	101
2024 Outreach and Coordination	
Notifications ⁵ and Briefings to External Overseers	34
Interagency Coordination and Leadership Activities	38
External Outreach (Domestic and Foreign)	54
Total	126

³ CLPT education and training include instances of civil liberties and privacy training during new employee orientation, privacy training provided by CLPT staff to the Federal Privacy Council, and small group sessions.

⁴ CLPT Oversight Reviews include in person and virtual reviews of intelligence activities, such as the implementation of FISA 702.

⁵ Notifications include sharing of light redacted Foreign Intelligence Surveillance Court (FISC) opinions and Section 702 procedures with Privacy and Civil Liberties Oversight Board (PCLOB).

Review, Advice, Assessment, Training, and Oversight Activities

In 2024, CLPT assisted IC agencies in numerous ways that implicated civil liberties, privacy, and transparency equities. The following material describes instances in which CLPT offered review, advice, assessment, training, and oversight related to these matters.

Commercially Available Information

During the reporting period, the DNI issued the IC CAI Policy Framework. This effort was led by ODNI's OGC, the Open Source Intelligence Executive, and CLPT, with extensive input and coordination from mission experts, OGCs, and CLPOs across the IC. The framework provides IC-wide guidance for cataloguing CAI acquired by IC elements to ensure that information about CAI holdings is accessible within the U.S. Government, as appropriate, in a manner that is consistent with relevant legal, security, classification, access control, and privacy considerations. The framework also includes principles that govern the IC's access to, collection, and processing of all CAI.

The framework represents the culmination of deliberate work to study this issue, including the DNI convening a Senior Advisory Group Panel that issued recommendations. Specifically, the Panel recommended that the IC: (1) develop a process to catalog the CAI that IC elements acquire; (2) develop a set of standards and procedures for CAI, governing and requiring regular reevaluation of acquisition and use decisions; and (3) develop more precise guidance to identify and protect sensitive CAI that implicates privacy and civil liberties concerns. Every IC element head reviewed and accepted the Panel's recommendations. Accordingly, the framework reflects the implementation of these recommendations.

The framework augments each IC element's Attorney General Guidelines and establishes a common baseline for how the IC accesses, collects, and processes CAI, while allowing individual IC elements the flexibility to operate in the manner best suited to meet their mission needs and protect privacy and civil liberties.

CNSS Privacy Overlays

On 31 October 2024, the CNSS issued its revised Privacy Overlays guidance, replacing the guidance issued in 2015. These 2024 Privacy Overlays provide a consistent, system-level privacy risk analysis process and a selection of relevant privacy controls to reduce privacy risks for national security systems (NSS), protect personally identifiable information (PII), and enable interagency trust and systems interoperability across the IC for NSS with PII. This revised guidance improves the 2015 guidance by modernizing the factors used to analyze the privacy risk of PII processed by NSS and closing loopholes to ensure that the IC protects all PII in NSS. The issuance of the Privacy Overlays is the result of a multi-year, multi-agency initiative co-led by the Director of Civil Liberties, Privacy, and Transparency at the National Security Agency and the Civil Liberties Protection Officer at ODNI.

CLPT supported our partners in numerous other ways. For instance, CLPT:

- Supported Congressional and public engagement on the re-authorization of Section 702 of FISA, which was reauthorized for two years starting 20 April 2024 under the Reforming Intelligence and Securing America Act (RISAA). CLPT reviewed a number of proposals related to the re-authorization of Section 702 of FISA and provided feedback on the possible civil liberties or privacy impacts of various proposals.
- Worked closely with the DOJ and IC elements to oversee the implementation of the new Section 702 requirements enacted in RISAA.
- Reviewed relevant Intelligence Community Directives (ICD) to ensure they fully addressed privacy and civil liberties concerns.
- Reviewed the IC Chief Data Officers' Council's charter and ODNI Data Management Strategy 2024-2028, ensuring the integration of civil liberties and privacy equities in carrying out data collection, exploitation, and dissemination, informing key initiatives in artificial intelligence and machine learning.
- Advised the newly formed IC Chief Artificial Intelligence Officer Council using the Artificial Intelligence Ethics Framework for the Intelligence Community (June 2020) and the Principles of Artificial Intelligence (AI) Ethics for the Intelligence Community (September 2022).

CLPT's Advice to ODNI, Review of ODNI Activities, and Related Training

In addition to providing reviews, advice, and assessments for IC-wide activities, CLPT provided guidance to ODNI Directorates, Components, and Offices. In 2024, CLPT had embedded personnel in three ODNI centers: the National Counterterrorism Center (NCTC); the National Counterintelligence and Security Center (NCSC); and the Foreign Malign Influence Center (FMIC). CLPT also assigned points of contact to the Chief Operating Officer and the Intelligence Advanced Research Projects Activity (IARPA). Having CLPT personnel dedicated to these offices ensured that CLPT could provide timely privacy and civil liberties guidance at early stages of proposed intelligence activities. CLPT's embedded personnel are well-known to the centers' personnel and facilitate continual informal checks with CLPT in addition to more formal requests for guidance.

CLPT revamped its Entry on Duty and Senior National Intelligence Service (SNIS) training for new government and joint duty-assigned employees, ensuring they become active participants in safeguarding civil liberties and privacy within their work centers. CLPT, in concert with OGC, developed train-the-trainer materials and updated existing agency-wide training on ODNI's Attorney General Guidelines. This effort enhances ODNI's protection of U.S. person information in the conduct of the agency's intelligence activities.

NCTC

NCTC's mission is to lead the nation's effort to protect the United States from terrorism by integrating, analyzing, and sharing information to drive whole-of-government actions and achieve national counterterrorism objectives.⁶

The NCTC CLPO advised NCTC on civil liberties, privacy, and transparency throughout the intelligence lifecycle. This includes:

- Membership on the NCTC Data Governance Board, where key decisions about data are made.
- Training of NCTC personnel on privacy and civil liberties.
- Review of acquisition, handling, use, and retention of data, as required under E.O. 12333 Attorney General Guidelines.
- Review of NCTC analytic products concerning domestic terrorism to ensure protection of U.S. persons' privacy and their exercise of constitutional rights in conformance with NCTC-CLPO Policy 1.
- Review of possible compliance incidents reported to, or discovered by, the NCTC Compliance & Transparency Group, which allow NCTC CLPO to identify systematic compliance issues and trends that could impact privacy, civil liberties, and transparency.
- Leading interactions between NCTC and the PCLOB. During the reporting period, PCLOB completed a report on NCTC as well as a report on the Terrorist Watchlisting process, which had NCTC equities.

NCSC

NCSC's mission is to lead and support the U.S. Government's counterintelligence and security activities critical to protecting the nation; provide counterintelligence outreach to U.S. private sector entities at risk of foreign intelligence penetration; and issue public warnings regarding intelligence threats to the United States.⁷

The NCSC CLPO provided advice to NCSC on issues, including:

- Addressing privacy and civil liberties concerns and implications related to the development of a new policy in response to an aspect of the Consolidated Appropriations Act of 2022⁸, which requires an implementing directive for sharing

⁶ The NCTC mission statement is available at <https://www.dni.gov/index.php/nctc-who-we-are>.

⁷ The NCSC mission statement is available at <https://www.dni.gov/index.php/ncsc-who-we-are/ncsc-mission-vision>.

⁸ Pub. L. No. 117-103, 136 Stat. 49 (2022).

covered insider threat information about contractor employees in the national security workforce. This work is ongoing.

- Ongoing development of privacy risk assessments and statutorily required system of records notices (SORN) for NCSC information systems, including revising the SORN for a system that fosters integration and coordination across the whole of government regarding activities such as evaluating the actual or potential damage to national security resulting from unauthorized disclosures of classified information.
- Continued development of the Trusted Workforce 2.0 initiative, including ongoing development of an annual vetting questionnaire and developing a new SORN for the Trusted Workforce programs.

Other ODNI Directorates, Components, and Offices

CLPT conducted regular reviews to ensure that privacy and civil liberties controls were properly applied within ODNI, including:

- Working with system owners and security personnel to evaluate the privacy risks of new or substantially updated ODNI systems and identify appropriate privacy controls to manage such risks.
- Reviewing reports of potential breaches involving PII and directing any necessary remedial efforts.
- Evaluating proposed programs and regularly reevaluate existing programs funded by IARPA to ensure that appropriate privacy and civil liberties controls are applied in all funded research activities.
- Working with FMIC to ensure privacy and civil liberties are protected in products used for partner engagements with the public and private sectors, as well as in documents identifying attributors of foreign information operations.

CLPT's Advice to U.S. Government-Wide Efforts

Artificial Intelligence: CLPT provided feedback on behalf of the IC to government-wide efforts seeking IC review. CLPT continued to promote awareness of the Principles of AI Ethics and AI Ethics Framework to advance the technical discussion and the responsible use of technology, ensuring continued focus on privacy and civil liberties protections.

Data Privacy Frameworks and Executive Order 14086: CLPT continued to provide feedback on U.S. Government work relating to implementing the national security aspects of the DPFs and complying with the requirements of E.O. 14086. Specifically, CLPT engaged in the following efforts:

- *Joint Review of the EU-U.S. DPF:* During the reporting period, CLPT supported the EU-U.S. Joint Review of the implementation of the DPF.

- *Designation of a Qualifying State:* CLPT supported the designation of Switzerland as a qualifying state.
- *Redress Mechanism:* E.O. 14086 provides a process for individuals in designated countries, who have a DPF, to submit complaints concerning IC SIGINT activities. CLPT activities to implement the redress mechanism included the following during the reporting period:
 - All practical aspects to implement the redress mechanism, including:
 - Creating technical processes with appropriate U.S. Government agencies and with appropriate public authorities to ensure that complaints and relevant communications are securely transmitted, which includes the secure transmission of qualified complaints.
 - Reviewing, updating, and developing CLPT internal policies and procedures concerning the redress mechanism.
 - Working with IC elements to implement their internal procedures for responding to the CLPO's request to access information concerning a submitted qualified complaint.
 - Engagement with appropriate public authorities (i.e., international data privacy authorities) to advance understanding of the redress mechanism. For example, CLPT reviewed documents for accuracy in describing the ODNI CLPO redress mechanism consistent with E.O. 14086 and ICD 126. Further, CLPT facilitated greater understanding by the international community of the redress mechanism through virtual and in-person meetings.
 - Reviewing a complaint transmitted to the CLPO by an appropriate public authority in a qualifying state that the CLPO determined to be the first qualifying complaint. Pursuant to the E.O. 14086 and ICD 126, the CLPO began an investigation and review of the qualifying complaint.

Intelligence Oversight

E.O. 12333 Guidance and Oversight

E.O. 12333 authorizes, guides, and limits activities conducted by the IC.⁹ This report focuses on the sections of E.O. 12333 that establish specific requirements to protect the civil liberties of U.S. persons.

⁹ See *generally* Exec. Order No. 12333, 46 Fed. Reg. at 59,941 (Dec. 4, 1981).

During the reporting period, CLPT:

- Conducted a review to understand how agencies report potential violations of E.O. 12333 and evaluated the data reported to the IOB by IC elements for trends. This work is still in progress.
- Began a review of IC activities conducted under E.O. 12333. This work is still in progress.
- Collaborated with OGC to provide oversight reporting to the IOB. These duties included reporting potential intelligence compliance issues to the IOB, evaluating the IOB incident submissions and submission processes of other IC elements for possible trends, meeting with the IOB, and facilitating and speaking at an IOB conference.

FISA Joint Oversight

CLPT, in partnership with OGC, the ODNI Mission Integration Directorate (MI), and DOJ, conducted joint oversight of the IC's use of Section 702 of FISA. Furthermore, CLPT, in coordination with OGC, MI, and DOJ, tracked the IC's implementation of RISAA reforms. CLPT's efforts resulted in stronger compliance with Section 702 requirements through oversight and advanced accountability to external overseers and the public.

- CLPT participated in eight on-site reviews of IC compliance documentation and guidance and worked with DOJ to identify, resolve, and report incidents of noncompliance to the Foreign Intelligence Surveillance Court (FISC) and Congress.
- CLPT participated in or led, in coordination with OGC and MI, interagency working groups monitoring the implementation of policy guidance for compliance with Section 702 requirements.
- CLPT led a working group, along with DOJ and the Federal Bureau of Investigation (FBI), to facilitate compliance with rules and procedures for the FBI's querying of Section 702-acquired information.

CLPT's FISA oversight activities are extensively documented in multiple *Semiannual Assessments of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, submitted by the Attorney General and the Director of National Intelligence (Joint Assessment) and available at www.intel.gov. Participating in such oversight efforts provided CLPT with visibility into compliance trends and equipped it with the factual information necessary to provide policy recommendations. These efforts also offered guidance to advance oversight and promote best practices to protect civil liberties and privacy.

Intelligence Transparency, Engagement, and Outreach

International Privacy Forum

CLPT facilitated in-depth conversations on how European and United States IC elements protect data privacy in their intelligence activities. CLPT hosted FVEY and European intelligence services at the 1st Annual International Intelligence Privacy Forum. This collaborative forum marked the first time intelligence services gathered to discuss privacy safeguards and transparency. The event provided a space to share insights on opportunities and challenges in data privacy, maintaining safeguards through training and technology, engaging with data protection authorities, and enhancing intelligence transparency.

Intelligence transparency is integral to the execution of CLPT's duties. It encompasses outreach and engagement with domestic and foreign partners, overseers and the public, as well as the public release of documents. CLPT has developed or supported efforts across the IC to explain the IC's mission, activities, authorities, and oversight mechanisms in a clear, concise, and effective manner. CLPT's championing of this type of proactive transparency advances the *Principles of Intelligence Transparency*, enhancing public understanding while protecting classified information.

CLPT routinely meets with foreign and domestic partners to describe the civil liberties and privacy protections embedded in the IC's activities; to detail the IC's initiatives to enhance transparency regarding its mission, authorities, and oversight mechanisms; and to learn from foreign partners about the comparable protections and programs they have instituted in the service of common democratic values.

CLPT organizes and engages directly with various government audiences, the public, academics, the private sector, and NGOs. Hosting:

- *Data Privacy Day*: CLPT held a town hall event in honor of Data Privacy Day to raise awareness about the importance of respecting privacy, safeguarding data, and fostering trust.
- *The 7th Annual U.S. IC CLPT Summit*: CLPT hosted members of the IC, U.S. Government, FVEY, European intelligence services, and oversight bodies, and representatives from foreign institutes for the 7th Annual U.S. IC CLPT Summit. The theme of this year's summit highlighted the importance of building and maintaining trust and leading the integration of civil liberties and privacy protections into the use of new technologies.
- *DNI Roundtable Discussions*: CLPT continued to support the DNI in her outreach to a broad spectrum of academic, private sector, and civil society groups, bringing in expertise and perspectives that are less frequently considered in the IC to identify ways to improve operations. These discussions ranged from topics on the IC Information Technology strategy to the Ethics of Intelligence and the CAI framework.

- *Federal Privacy Council:* CLPT continued to contribute to government-wide efforts by participating in FPC-sponsored panels and other trainings designed to increase the privacy acumen of professionals throughout the U.S. Government. CLPT also co-led the Agency Implementation Committee, which hosts educational sessions each month for 140–160 federal privacy professionals on key privacy topics, including reporting privacy breaches, assessing artificial intelligence, and incorporating privacy into contracts.

Other ways in which CLPT engaged included speaking at different forums such as:

- *Department of Commerce:* CLPT's Chief participated in a two-day joint EU-U.S. DPF Joint Review, which covered both commercial and national security commitments. The CLPT Chief led the second day, which covered the implementation of E.O. 14086 by IC elements and the redress mechanism. The DOJ and State Department also participated.
- *Privacy Symposium 2024:* CLPT's Chief spoke about privacy and redress in the national security context.
- *Meetings with European Data Protection Authorities:* CLPT's Chief had two separate meetings regarding the redress complaint mechanism under E.O. 14086 and the EU-U.S. DPF.
- *Panel Discussion:* CLPT's Chief spoke on a panel about the CLPO redress complaint mechanism and other IC privacy safeguards and oversight regimes during a public conference hosted by the European Data Protection Supervisor (EDPS) in Europe.
- *Outreach Efforts:* CLPT conducted extensive outreach to foreign partners, oversight entities, academia, civil society, and the public regarding the work of the IC. As noted above, there was particular focus on the DPF and the CLPO redress function. Overall, CLPT's global public engagements concerning intelligence oversight and data privacy improved public understanding and trust in U.S. intelligence collection practices.
- *Global Privacy Assembly:* CLPT continued its observer status in the Global Privacy Assembly, a global forum for over 130 data protection and privacy authorities to engage and lead on the topics of data protection and privacy worldwide. CLPT's participation provided a unique opportunity to share the IC's privacy safeguards with global data privacy officials and explain the new ODNI CLPO redress mechanism.
- *Speaking Engagement:* The Deputy CLPT spoke at the International Association of Privacy Professionals Asia Conference alongside the DOC and others on the implementation of the Organization for Economic Cooperation and Development (OECD) Trusted Government Access Principles (TGA).

- *Training Session:* CLPT joined a representative from the DOC's International Trade Administration to educate a group of State Department cyber and digital policy officers from around the world about the *Role of Governments in Securing Data and Protecting Privacy*. This session was part of State's inaugural combined training for these officers to develop their ability to effectively engage with foreign government and private sector stakeholders on cyber and digital policy topics. While the DOC representative shared insights about the wider USG approach and commercial perspectives, CLPT focused on the national security perspective of government access to data. CLPT highlighted the emergence of national security concerns in the global data privacy conversation and discussed current trends related to the new EU-U.S. DPF, E.O. 14086, and principles in the Organization for Economic Cooperation and Development's (OECD) Trusted Government Access declaration.

CLPT has also championed and facilitated the IC's transparency to the public through authorized releases, whether such releases are required by statute or proactive:

- *Annual Statistical Transparency Report:* CLPT led and published the Annual Statistical Transparency Report (ASTR), which details how the government uses FISA and other authorities to fulfill the mission of the Intelligence Community. In addition to presenting statistics on various authorities used by the IC, which are declassified for public release by the DNI, the ASTR includes robust explanations about FISA authorities to enhance public understanding consistent with the Principles of Intelligence Transparency.¹⁰
- *FISC Opinion:* The ODNI publicly released a 2024 FISC Opinion on FISA Section 702 Recertifications, which approves the annual certifications submitted by the DNI and the Attorney General (AG) pursuant to Section 702 of FISA, along with the associated targeting, minimization, and querying procedures as defined in FISA.¹¹
- *Intel.gov:* CLPT's extensive transparency efforts aim to facilitate the IC's adherence to the democratic value of accountability to the public. The IC must both follow the rule of law and ensure that relevant overseers and the public understand the governing authorities, rules, and compliance with those requirements. During this reporting period, CLPT led the release of guidance discussing how to harness AI to fulfill national security objectives. CLPT also released "Podcasts from the IC." which provide the public with unique perspectives on global affairs, cybersecurity, and more.¹²
- *E.O. 14086:* CLPT released public documents (a slide deck, postcard, and frequently asked questions) and participated in numerous public conferences and

¹⁰ The Annual Statistical Transparency Report for calendar year 2023 is available at <https://www.intel.gov/astr>.

¹¹ These documents are available at <https://www.intel.gov/ic-on-the-record-database>.

¹² Harnessing Artificial Intelligence to Fulfill National Security Objectives is available at <https://www.intel.gov/ai>, and Podcasts from the IC is available at <https://www.intel.gov/publics-daily-brief#podcastPage>.

robust engagements with international partners to advance public awareness and broaden their understanding of the redress mechanism. Additionally, during the reporting period, CLPT engaged with international partners, particularly their data protection authorities, to facilitate a clear understanding among authorities and enhanced public awareness. This included both virtual and in-person meetings.

Transparency to External Overseers

CLPT continued to lead the IC in maintaining transparency to external overseers. CLPT facilitated ongoing oversight of Section 702 and other intelligence authorities by Congress and the PCLOB through coordinating and supporting the ongoing production of classified FISA documentation, interagency responses to questions from those overseers, and briefings on the mission use, value, and privacy and civil liberties controls of the Section 702 program. For example, the PCLOB and Congress received the classified versions of the 28th and 29th Joint Assessments. As a result of these transparency efforts, IC overseers became better informed about the IC's use of important surveillance authorities.

The Intelligence Community Civil Liberties and Privacy Council and the Intelligence Transparency Council

Consistent with the role of ODNI in integrating intelligence activities across the IC, CLPT leads two IC councils: (1) the IC CLP Council and (2) the ITC. These councils facilitate collaboration between the IC civil liberties, privacy, and transparency officers, contributing to efforts that significantly advance civil liberties, privacy protections, and transparency.

During the reporting period, the IC CLP Council focused on privacy and civil liberties safeguards in AI and in cataloging of CAI.

The ITC continued its proactive transparency efforts to further ODNI's transparency goals. Additionally, a small group was formed to develop FISA-related review, redaction, and release procedures that formalize efforts related to classified Congressional and PCLOB productions, as well as authorized public releases.

Complaints

CLPT ensures there is an avenue for redressing complaints, addressing concerns, or answering questions related to privacy and civil liberties, whether broadly focused (e.g., the privacy implications of intelligence activities) or tied to specific, individual concerns (e.g., how a particular personnel record may have been used).

During the reporting period, CLPT received and processed eight complaints, four of which did not qualify as formal complaints, also known as non-qualifying complaints. In addition to these complaints, CLPT routinely addressed broader privacy and civil liberties concerns and questions raised by IC personnel, other government personnel, or members of

the public. The existence of CLPT's program for the review and evaluation of formal complaints strengthens privacy and civil liberties oversight across the IC.

While the details of formal complaints generally remain anonymous to protect the confidentiality of the complainants, the eight complaints can be described as follows:

- CLPT reviewed and processed two of these complaints and determined they were valid privacy and/or civil liberties complaints. CLPT provided one or more recommendations to other ODNI offices and, in some cases, engaged with the subject offices to improve privacy processes or policies. Additionally, CLPT reviewed and processed four privacy or civil liberties complaints and determined they were not valid. However, these complaints highlighted the need for enhanced CLPT advisory engagement and public awareness. CLPT's investigation of two complaints received during the reporting period that involved civil liberties remained open at the end of the period. Portions of these complaints involved coordination and engagement with one or more offices, which remained ongoing at that time.

CLPT continues its work to inform the ODNI workforce, through in-person sessions and CLPT websites, that anyone can report a potential civil liberties and privacy violation and how to submit a complaint or raise a concern. IC and ODNI personnel may submit complaints and concerns to CLPT by visiting CLPT offices or contacting CLPT via telephone, email, and CLPT's intra-IC website. During this reporting period, CLPT established an ASKCLPT email account available to IC and ODNI personnel to help manage complaint inquires and respond to questions and concerns more efficiently.

Individuals outside of the IC (as well as those inside the IC) may submit a written complaint to CLPT, provided it does not contain any classified information, to the following address:

Office of the Director of National Intelligence
ATTN: Office of Civil Liberties, Privacy, and Transparency
Washington, DC 20511

Further, CLPT ensures that the IC and ODNI workforce understands they will be protected from retaliation when bringing allegations of civil liberties and privacy abuses to CLPT. Specifically, no action constituting a reprisal or threat of reprisal may be made against a federal employee for making a complaint or for disclosing information to CLPT that indicates a possible violation of civil liberties or privacy protections in the administration of ODNI programs and operations, unless the complaint is made or the information is disclosed with the knowledge that it is false or made with willful disregard for its truth or falsity.

Complaints Submitted Per E.O. 14086

As discussed above, E.O. 14086 creates a SIGINT redress mechanism with two levels of independent redress. The first level requires that the independent ODNI CLPO investigate, review, and, as appropriate, determine remediation of qualified complaints transmitted by an appropriate public authority of a qualifying state. During the reporting period, the Attorney General designated Switzerland as a qualifying state.¹³

One complaint was transmitted to the ODNI CLPO on 3 December 2024, from the Austrian DPA via the appropriate public authority for the EU, the EDPB. Upon review, the CLPO assessed that the complaint qualified under the requirements of E.O. 14086 and provided notice to the EDPB, the DOC, and the Data Protection Review Court as required by IC Directive 126. CLPT implemented internal operating processes to facilitate the CLPO's investigation and review of the complaint.

¹³ On 7 June 2024, the Attorney General designated Switzerland as a "qualifying state" for purposes of implementing the redress mechanism established in E.O. 14086. This designation became effective on 15 September 2024. See *generally* <https://www.justice.gov/opcl/executive-order-14086>.

Metrics

Complaints Relating to the Privacy Act and Privacy and Civil Liberties (Not Submitted Under E.O. 14086)

Table 2: Number of Complaints Relating to Privacy and Civil Liberties

	No Privacy or Civil Liberties Matter Identified	Privacy or Civil Liberties Matters Identified and an Investigation Started	Complaint Resolved
Privacy Act Complaint	0	1	1
Privacy and Civil Liberties Complaint	5	3	1
Totals	5	4	2

CLPT used the following definitions to calculate these metrics:

- Privacy Act Complaint:** Refers to complaints submitted to CLPT alleging ODNI non-compliance with a requirement of the Privacy Act of 1974 (5 U.S.C. § 552a). Per 50 U.S.C. § 3029(b)(5), the CLPO must ensure that personal information is handled in compliance with the Privacy Act. Complaints covered by this category include allegations that an ODNI office improperly retained or disseminated an individual's personally identifiable information (such as a social security number).
- Privacy and Civil Liberties Complaint:** Refers to complaints submitted to CLPT alleging a violation of privacy rights and civil liberties. The CLPO has the duty to review and assess complaints indicating possible abuses of civil liberties and privacy in ODNI's administration of programs and operations. See 50 U.S.C. § 3029(b)(3); 42 U.S.C. § 2000ee-1(a)(3); ODNI Instruction 80.13. Complaints covered by this category include, for example, allegations relating to improper collection, use, retention, and dissemination of information about U.S. persons; violations of First Amendment rights of free speech and association; or Fifth Amendment guarantees of due process and equal protection.
- No Privacy or Civil Liberties Matter Identified:** Refers to complaints submitted to CLPT where the CLPO determined that the complaint did not contain a matter related to the Privacy Act, privacy, or civil liberties and, thus, the CLPO did not initiate an investigation. When such complaints include matters relating to the competency of another ODNI oversight office (e.g., ODNI's Equal Employment

Office for complaints alleging employment discrimination), the CLPO directs the complainant to the appropriate oversight office.

- **Privacy or Civil Liberties Matter Identified:** Refers to complaints submitted to CLPT where the CLPO determined that the complaint did contain a matter related to the Privacy Act, privacy, or civil liberties and, thus, the CLPO initiated an investigation.
- **Complaint Resolved:** Refers to complaints where the CLPO started an investigation and concluded the investigation.

Complaints Submitted Under E.O. 14086

Table 3: Number of Complaints Related to the ODNI CLPO Redress Mechanism

	Non-Qualifying Complaints	Qualifying Complaints	CLPO Review Completed and Notice Given
Properly Submitted Complaints	0	1	0
Improperly Submitted Complaints	0	N/A	N/A
Totals	0	1	0

CLPT used the following definitions to calculate these metrics:

- **Properly Submitted Complaints:** Refers to complaints that are “transmitted [to the CLPO] by the appropriate public authority in a qualifying state,” as required by E.O. 14086 Sections 3(a). After receipt of the properly transmitted complaint, the CLPO must assess whether the complaint qualifies under E.O. 14086 Section 4(k). *Thus, properly submitted complaints may be qualifying or non-qualifying.*
- **Improperly Submitted Complaints:** Refers to complaints that are not “transmitted [to the CLPO] by the appropriate public authority in a qualifying state,” as required by E.O. 14086 Section 3(a). Such improperly transmitted complaints would include those submitted directly to the CLPO by the complainant or by another entity. *All improperly transmitted complaints are non-qualifying and, thus, the CLPO will not begin an investigation. There cannot be any pending or completed review for non-qualifying complaints, and no review by the Data Protection Review Court (DPRC).* Hence, the chart indicates “N/A” (*i.e.*, non-applicable) for those cells.
- **Non-Qualifying Complaints:** Refers to complaints that are (a) not properly transmitted to the CLPO or (b) properly transmitted but assessed by the CLPO as not meeting the requirements of E.O. 14086 Section 4(k) to be qualifying.

- **Qualifying Complaints:** Refers to complaints that (a) have been properly submitted to the CLPO (*i.e.*, transmitted by the appropriate public authority in a qualifying state), (b) the CLPO assessed to be qualifying under E.O. 14086 Section 4(k), and (c) for which the CLPO accordingly initiated an investigation under E.O. 14086 Section 3(c)(i)(A).
- **CLPO Review Completed and Notice Given:** Refers to qualifying complaints where the *CLPO* (a) *completed investigation and review* under E.O. 14086 Sections 3(c)(i)(A)–(D), and (b) provided notice to *the complainant, through the appropriate public authority in a qualifying state*, that the review was completed, as required by E.O. 14086 Section 3(c)(i)(E).

Conclusion

As required by Section 1062 of IRTPA, this report provides information about CLPT’s activities from 1 January 2024 to 31 December 2024. These activities continue to assist the ODNI and the IC in meeting their obligations to the American people by ensuring that intelligence activities are conducted in a manner that protects privacy and civil liberties while promoting transparency and accountability.

Appendix: Acronyms/Abbreviations

ACRONYM/ ABBREVIATION	DEFINITION
AG	Attorney General
AI	Artificial Intelligence
ASTR	Annual Statistical Transparency Report
CAI	Commercially Available Information
CLPC	Civil Liberties and Privacy Council
CLPO	Civil Liberties Protection Officer
CLPT	Office of Civil Liberties, Privacy, and Transparency
CNSS	Committee on National Security Systems
DOC	Department of Commerce
DOJ	Department of Justice
DPA	Data Protection Authority
DPF	Data Privacy Framework
DPRC	Data Protection Review Court
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FMIC	Foreign Malign Influence Center
FPC	US Federal Privacy Council
FVEY	Five Eyes
IARPA	Intelligence Advanced Research Projects Activity
IC	Intelligence Community
ICD	Intelligence Community Directives
IOB	Intelligence Oversight Board
IRTPA	Intelligence Reform and Terrorism Prevention Act
ITC	Intelligence Transparency Council

ACRONYM/ ABBREVIATION	DEFINITION
MI	Mission Integration
N/A	Not Applicable
NCSC	National Counterintelligence and Security Center
NCTC	National Counterterrorism Center
NGO	Non-Governmental Organization
NIPF	National Intelligence Priorities Framework
NSS	National Security Systems
ODNI	Office of the Director of National Intelligence
OECD	Organization for Economic Cooperation and Development
OGC	Office of General Council
PCLOB	Privacy and Civil Liberties Oversight Board
PII	Personally Identifiable Information
RISAA	Reforming Intelligence and Securing America Act
SIGINT	Signals Intelligence
SNIS	Senior National Intelligence Service
SORN	System of Records Notice
TGA	Trusted Government Access
U.S.C.	United States Code
USG	United States Government