



## INTELLIGENCE COMMUNITY DIRECTIVE

505

UNCLASSIFIED

### Artificial Intelligence

---

**A. AUTHORITY:** The National Security Act of 1947, as amended; Section 6702 of the Intelligence Authorization Act for Fiscal Year 2023, as amended; Executive Order 12333, as amended; and other applicable provisions of law.

**B. PURPOSE**

1. This Intelligence Community Directive (ICD) establishes policy on governance and management of the artificial intelligence (AI) developed, acquired, or used by or on behalf of the Intelligence Community (IC).

**C. APPLICABILITY**

1. This Directive applies to the IC, as defined by the National Security Act of 1947, as amended, and to such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned, as an element of the IC.

a. With the exception of section D.5.b., this Directive does not apply to AI that (1) is generally available to the public without charge; (2) is accessed under the same terms as are available to the public; (3) has not been modified by any element of the IC; and (4) is used in accordance with applicable laws and policies.

b. This Directive does not apply to the testing and evaluation of a potential vendor, commercial capability, or freely available AI capability for the purpose of making a procurement or acquisition decision, so long as the capability is not otherwise used in IC element operations.

c. For IC elements that are also a component of a Department, this Directive does not apply to AI that is made available by their Department, is not used for intelligence purposes, and is not hosted on IC networks.

**D. POLICY**

1. AI offers extraordinary potential to advance the work of the IC. The IC must govern, manage, and oversee AI to accelerate and increase its adoption and enhance its interoperability while maintaining the IC's commitment to the Constitution and rule of law and to responsible and ethical AI.

UNCLASSIFIED

a. Consistent with 15 U.S.C. 9401(3), and for the purposes of this policy, the term AI means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. AI systems use machine- and human-based inputs to (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action.

b. This ICD advances the goals and direction in *Memorandum on Advancing United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security and Trustworthiness of AI* (National Security Memorandum-25 [NSM-25]), issued 24 October 2024, and companion document *Framework to Advance AI Governance and Risk Management in National Security* (AI Framework), issued 24 October 2024.

## 2. Governance

a. The DNI shall designate an IC Chief AI Officer (CAIO) to establish and oversee the strategic direction of AI for the IC. The IC CAIO shall establish IC AI governance practices that accelerate and increase the deployment and adoption of responsible and ethical AI throughout the IC consistent with applicable law and policy.

(1) The IC CAIO shall coordinate and collaborate, as appropriate, with:

(a) The IC Chief Information Officer (CIO) to ensure the IC Information Environment enables implementation of AI and that proposed IC AI guidance is consistent with IC CIO guidance.

(b) The IC Chief Data Officer (CDO) to ensure:

(i) Data is managed and data tradecraft is implemented throughout the lifecycle of IC AI.

(ii) Proposed IC AI guidance is consistent with IC CDO guidance.

(c) The ODNI Civil Liberties and Privacy Officer (CLPO) to ensure:

(i) Guidance issued under this Directive protects privacy and civil liberties;

(ii) Consistent with ICD 107, *Civil Liberties, Privacy, and Transparency*, civil liberties, privacy, and transparency are appropriately incorporated into the AI-related procedures of IC elements; and

(iii) IC AI activities related to civil liberties, privacy, and transparency are reported appropriately.

(d) The Chief, IC Diversity, Equity, Inclusion, and Accessibility (DEIA) to ensure compliance with relevant non-discrimination and accessibility laws and policy.

(2) The IC CAIO shall guide and advocate for IC AI interoperability.

(a) IC AI interoperability shall be enabled by common IC AI guidance issued under this ICD; legal and policy requirements; common data management practices, consistent

with ICD 504, *IC Data Management*; and information technology interoperability in the IC Information Environment, consistent with ICD 121, *Managing the IC Information Environment*.

(b) The IC CAIO shall maximize AI interoperability with external mission partners and stakeholders, including the Department of Defense (DoD); other U.S. Government departments and agencies; state, local, tribal, and territorial governments; foreign partners; and the private sector. This includes facilitating sharing of AI with partners, when appropriate and in compliance with existing policy and guidance.

(3) The IC CAIO shall strive to consolidate and collaborate on IC AI efforts with DoD, as practical and as appropriate.

b. Mitigation of unintended bias is critical to accelerating and increasing adoption of AI. The IC CAIO shall coordinate with the IC CDO, the ODNI CLPO, the Chief, IC DEIA, and relevant experts from ODNI Mission Integration, as appropriate, on addressing unintended bias issues.

(1) Consistent with law and policy, to include relevant Equal Employment Opportunity laws and policies, unlawful discriminatory bias in IC AI is prohibited.

(2) Analytic bias is addressed in ICD 203, *Analytic Standards*, and implementing guidance.

c. Each IC element head shall identify and designate an IC element CAIO, in coordination with the IC CAIO on behalf of the DNI. IC element heads shall submit to the IC CAIO, in writing, the designation of their IC element CAIO within 30 days of signature of this Directive, and thereafter within 15 days of new designations. In IC elements with a mandated CAIO under Executive Order 14110, that CAIO may concurrently serve as the IC element CAIO. The IC CAIO shall maintain a record of those designated IC element CAIO. IC element CAIOs should be senior officials who shall, at a minimum, possess:

(1) Authority to speak on behalf of their IC element with regard to AI;

(2) Skills, knowledge, and expertise to perform the responsibilities described in this Directive;

(3) Insight into development, use, and acquisition of AI by or on behalf of their IC element, sufficient to execute the provisions of this Directive; and

(4) In the context of IC element AI, an understanding of protection of civil liberties and privacy as well as mitigation of unintended bias.

d. IC element CAIOs shall oversee and coordinate IC element efforts related to AI, including through integration of any acquisition, technology, human capital, and financial management aspects necessary for the adoption of AI.

e. Upon request, IC element CAIOs shall inform the IC CAIO about the progress, status, adoption, and management of AI within their IC element and the implementation of this Directive.

f. There shall be an IC CAIO Council. It shall be chaired by the IC CAIO and composed of IC element CAIOs. The IC CAIO Council shall focus on the strategic direction, governance, interoperability, and risk management of AI within the IC and shall serve as a forum to discuss, advise, advocate, and share knowledge, oversight approaches, and best practices.

(1) The ODNI Assistant Director for Acquisition, Procurement & Facilities; the ODNI Associate Deputy DNI for Mission Integration; the IC CDO; the IC Chief Financial Officer; the IC CIO; the IC Chief Information Security Officer; the ODNI CLPO; the Director, National Counterintelligence and Security Center; and IC Human Capital Officer (IC HC) shall serve as advisors to the IC CAIO Council.

### 3. Oversight

a. IC elements shall ensure oversight of AI, including associated hardware, software, and data, to prevent, identify, and mitigate the risk of violation of civil liberties and privacy protections and the presence of unintended bias.

(1) Each IC element shall establish and implement procedures to report misuse of AI internally to their IC element CAIO and to appropriate oversight offices, and externally including to the IC CAIO on behalf of the DNI, as appropriate.

(2) IC elements shall have supporting procedures for response to such reports, including procedures to receive complaints anonymously, when appropriate.

(3) AI users shall be notified of how to report concerns related to protecting civil liberties and privacy, AI input and AI-derived output unintended bias, or other matters to the appropriate oversight office.

b. AI may be trained and/or fine-tuned by or on behalf of an IC element, or an IC element may acquire AI that has already been trained and/or fine-tuned.

(1) IC elements shall only train or fine tune IC element AI, or have IC element AI trained or fine-tuned on their behalf, using synthetic data or data obtained or derived from, and used, in accordance with applicable law and policy. Examples of applicable law and policy include, but are not limited to, Executive Order 12333 and implementing Attorney General Guidelines, intellectual property law, the Privacy Act of 1974, and IC Policy Memorandum 504(01), *Intelligence Community Policy Framework for Commercially Available Information*.

(2) The IC CAIO shall issue guidance on AI trained or fine-tuned using data that potentially contains U.S. person information, publicly available information, commercially available information, or intellectual property. This guidance shall be coordinated with the IC CDO and the ODNI CLPO. IC elements shall implement the guidance.

c. Use of AI to analyze data that either includes U.S. person information as an input or that may result in U.S. person information as an AI output requires additional guidance. The IC CAIO, in coordination with the IC CDO and the ODNI CLPO, shall establish guidance addressing that topic. IC elements shall implement the guidance. This guidance shall apply in addition to and shall not conflict with any requirements established through Executive Order 12333 and implementing Attorney General Guidelines. Attorney General Guidelines shall have primacy if there are real or perceived inconsistencies.

d. IC elements shall, in consultation with their IC element senior official responsible for privacy and civil liberties, develop and apply safeguards to IC element AI or associated software or data to ensure appropriate protection for civil liberties and privacy. At a minimum, these safeguards shall include adherence to IC guidance on AI ethics, such as the *AI Ethics Framework for the IC* and the *Principles of AI Ethics for the IC* or successor documents, and with the Privacy Act, as applicable.

e. IC elements shall perform impact assessments on IC element AI consistent with NSM-25, the AI Framework, and with the ODNI CLPO guidance developed in consultation with IC CAIO.

f. The ODNI CLPO shall periodically, but not less frequently than annually, submit a report to the DNI on their activities associated with AI oversight, including, for example, evaluations of risk management processes.

g. The IC CDO, in consultation with the IC CAIO and with the IC CDO Council, shall establish minimum standards for the documentation of data used to train AI developed, procured, or used by or on behalf of an element of the IC. At a minimum, standards shall be established for documentation of imputed, augmented, or synthetic data used to train IC AI.

#### 4. Accountability

a. IC element CAIO shall oversee IC element AI throughout the AI lifecycle, including the AI's disposition or removal from use.

b. IC elements, through the IC element CAIO, shall establish and implement processes for identifying accountability for and responding to unexpected, inaccurate, or unintentionally biased IC element AI outputs, including by:

- (1) Notifying users about how to provide feedback about IC element AI performance;
- (2) Receiving, responding to, and, as needed, mitigating AI performance outside of expected performance; and
- (3) Following applicable oversight reporting requirements.

c. IC element AI, including associated hardware, software, and data, shall be auditable for performance and compliance with relevant guidance, shall be periodically audited by the IC element, and those audit results shall be reviewable and verifiable by IC element personnel.

d. AI provenance shall be tracked and monitored throughout the AI's lifecycle. To facilitate this and to enhance shared insight into AI across the IC, the IC CAIO shall designate an IC AI model registry to serve as a central inventory for IC AI model information. The IC CAIO shall, in consultation with the IC CAIO Council, determine the content of IC AI registry entries and shall provide additional guidance as appropriate.

(1) Upon designation of the model registry, IC elements shall ensure that each IC element AI model is documented and registered in the IC AI model registry.

(2) The model registry and its contents shall be electronically discoverable and accessible to the IC, consistent with legal and policy requirements. For any AI model registry

entries exempt from discovery under IC Policy Guidance (ICPG) 501.1, *Exemption of Information from Discovery*, this requirement may be fulfilled via separate model registries.

#### 5. Risk Management

a. AI risk shall be governed to protect the IC's ability to perform its mission, consistent with ICD 503, *Intelligence Community Information Environment Risk Management*.

b. To manage AI risk across the IC, the IC CAIO, in consultation with the IC CAIO Council, shall establish an IC AI risk management framework for AI developed, acquired, or used by or on behalf of the IC. At a minimum, the IC AI risk management framework shall incorporate the risk management framework, AI use restrictions, and minimum risk management practices established in the NSM-25 and the AI Framework. IC elements shall identify, characterize, assess, and manage risk using the IC AI risk management framework

(1) The IC CAIO may, in consultation with the IC CAIO Council, add to the IC AI risk management framework. This includes but is not limited to additional AI use restrictions and minimum risk management practices.

(2) IC elements may issue waivers to minimum risk management practices identified in the IC AI risk management framework. IC elements shall report to the IC CAIO all waivers to minimum risk management practices within 3 days of issuance or renewal unless otherwise directed by the IC CAIO in accordance with applicable oversight guidance.

(a) The IC CAIO shall, upon receipt, make those waivers available to the ODNI CLPO.

(3) Each IC element shall maintain an inventory of their AI use cases and systems under AI use restriction as well as IC element approved waivers to minimum risk management practices, consistent with guidance issued by the IC CAIO. IC elements shall report the inventory and waivers to the IC CAIO upon request.

(4) IC CAIO guidance issued to implement section D.5.b. of this Directive shall be coordinated with the ODNI CLPO when related to civil liberties and privacy.

c. IC elements shall establish and implement a process to evaluate and approve proposals to accept a given AI for use or reuse and to ensure the AI is appropriate for their IC element's given use case.

(1) IC element personnel shall only use malicious techniques against IC element AI when preapproved by their IC element CAIO in pursuit of an authorized activity (e.g., testing).

d. When necessary to ensure compliance with this Directive and with other relevant guidance, IC element CAIOs shall be consulted during IC element accreditation and authorization processes for IC element capabilities that incorporate AI.

e. IC element testing and evaluation of IC element AI to identify unexpected performance shifts shall be ongoing or at a periodicity determined by the IC element to maintain necessary performance.

f. IC elements, through their IC element CAIOs, shall notify the IC CAIO of unexpected, upcoming, imminent, or ongoing changes to IC element AI, including changes derived from associated hardware, software, or data, which could significantly negatively affect another IC element's ability to conduct necessary business operations or could degrade performance of an assigned IC function. The IC CAIO shall share notifications with the IC CAIO Council as appropriate and may help facilitate resolution of any resulting mission execution concerns.

(1) IC elements shall provide notifications to the IC CAIO as far in advance as possible, but not less than 30 days before expected changes.

(2) For unexpected changes, IC elements shall notify the IC CAIO as soon as practicable.

(3) IC elements are encouraged to share and discuss change decisions with other affected IC elements prior to formal IC CAIO notification.

g. The IC CAIO shall, in consultation with the IC CAIO Council, establish procedures to share information within the IC and with DoD, at a minimum when an AI system developed, deployed, or used by a contractor demonstrates risks related to safety, security, and trustworthiness, including to human rights, civil rights, civil liberties, or privacy. Specific procedures for when risks potentially affect U.S. person civil rights and liberties and privacy will be coordinated with the ODNI CLPO.

#### 6. Centricity of IC Personnel

a. AI must enable and enhance the decisions of IC personnel as it becomes integral to the business and mission of the IC. IC personnel shall remain responsible and accountable for the analysis, decisions, and outcomes derived from insights gleaned using AI.

b. Recipients of IC data shall be informed, such as through a watermark, when they receive IC data produced or substantially influenced by IC AI, unless operational, sources and methods protection, or security considerations prevent notification.

(1) IC personnel shall understand appropriate use for each AI instance that they interact with and shall be accountable for adhering to it.

(2) IC personnel shall be able to review, challenge, and reject or replace AI-derived recommendations and findings when appropriate.

#### 7. IC Policy Implementation

a. IC element heads shall ensure that IC element AI complies with all applicable classification and handling requirements.

(1) All security classification of AI, its contents, its derived outputs, and its processes shall be established by an Original Classification Authority (OCA), consistent with law and policy, and may be documented through a Security Classification Guide. Derivative classifiers shall apply those OCA determinations. Considerations shall include classification by compilation.

(2) AI can potentially be changed or influenced by data that it has been exposed to, including classified data. To account for the protection of classified data, IC element CAIOs shall determine whether each IC element AI has the reasonable potential to reveal or recreate classified data to which it has been exposed by an authorized recipient of that intelligence.

(a) The IC CAIO, in consultation with the IC CAIO Council, shall develop best practices or other guidelines to help determine whether a given AI can reasonably reveal or recreate classified data to which it has been exposed.

(b) For AI with the reasonable potential to reveal or recreate classified data to which it has been exposed, AI output data shall be classified using the maximum level of classification and most restrictive control markings of all data to which the AI has been exposed. However, IC personnel may apply different classification and control markings for a given AI output, if warranted by established classification guidance.

(c) For AI assessed not to have the reasonable potential to reveal or recreate classified data to which it has been exposed, AI output data shall be classified consistent with comparable data developed without the use of AI.

(d) AI shall reside on information technology approved for the classification of the data that it is interacting with, the data that it has the reasonable potential to reveal or recreate, and the capabilities that the AI itself reveals.

(3) IC elements shall implement processes to ensure IC element AI outputs are classified appropriately.

(4) The IC CAIO shall work to align the IC's classification practices for AI and AI-derived outputs, as well as deconflict IC element determinations about whether a given AI has the reasonable potential to reveal or recreate classified data, in consultation with the ODNI Information Management Office and the Controlled Access Program Central Office.

b. AI and associated software shall be designed to comply with and, as appropriate and feasible, carry forward all handling requirements for data that it is used to analyze. Data traceability shall be maintained across AI inputs and AI-derived outputs to the maximum extent practicable.

c. When relevant, IC AI shall be designed and deployed to enable IC personnel to adhere to analytic standards, including those established in ICD 203 and ICD 206, *Sourcing Requirements for Disseminated Analytic Products*. To enable this requirement, data access provided to IC AI and access to IC AI-derived outputs shall adhere to the "responsibility to provide" principle established in ICD 501, *Discovery and Dissemination or Retrieval of Information Within the IC*. This requirement does not supersede exemptions from discovery established in accordance with ICPG 501.1 or governed in applicable law and policy.

#### 8. AI-Ready Workforce

a. To take advantage of AI and respond to quickly evolving demands, the IC workforce must be equipped with the awareness and expertise necessary to enable the implementation and utilization of responsible and ethical AI. The IC CAIO and the IC HC shall develop or identify, at a minimum, foundational and, as appropriate, advanced AI competencies, knowledge, and



skills for different roles within the IC. IC element heads shall ensure their workforce has the requisite foundational and, as appropriate, advanced AI-related competencies, knowledge, and skills.

#### **E. ROLES AND RESPONSIBILITIES**

1. The IC CAIO shall:
  - a. Advise the DNI on matters related to AI.
  - b. Serve as the accountable official for the implementation of this Directive.
  - c. Develop and promulgate IC Standards in accordance with IC Policy Guidance 101.2, *Intelligence Community Standards*, and other guidance as necessary to implement this Directive.
  - d. Establish and oversee the strategic direction of AI for the IC, and establish IC AI governance practices that accelerate and increase the deployment and adoption of responsible and ethical AI throughout the IC consistent with applicable law and policy.
  - e. Coordinate and collaborate with the IC CIO, the IC CDO, the ODNI CLPO, and the Chief, IC DEIA, as appropriate.
  - f. Guide and advocate for IC AI interoperability within the IC and with external mission partners and stakeholders, including by facilitating sharing of AI with partners when appropriate and in compliance with existing policy and guidance.
  - g. Strive to consolidate and collaborate on IC AI efforts with DoD, as practical and as appropriate.
  - h. Coordinate on unintended bias mitigation with the IC CDO, the ODNI CLPO, the Chief, IC DEIA, and relevant experts from ODNI Mission Integration, as appropriate.
  - i. Coordinate with IC element heads, on behalf of the DNI, on the designation of IC element CAIO, and maintain a record of those designated IC element CAIOs.
  - j. Solicit and collect input from IC element CAIOs about the progress, status, adoption, and management of AI within their IC element, and the implementation of this Directive.
  - k. Serve as Chair of the IC CAIO Council.
  - l. Issue guidance on the use of AI trained or fine-tuned using data that potentially contained U.S. person information, publicly available information, commercially available information, or intellectual property, in coordination with the IC CDO and the ODNI CLPO.
  - m. Issue guidance on the use of AI to analyze data that either includes U.S. person information as an input or that may result in U.S. person information as an AI output, in coordination with the IC CDO and the ODNI CLPO.
  - n. Consult with the IC CDO on establishing minimum standards for the documentation of data used to train any model developed, procured, or used by or on behalf of an element of the IC. At a minimum, standards shall be established for documentation of imputed, augmented, or synthetic data used to train IC AI.

- o. Designate an IC AI model registry for IC AI model information and, in consultation with the IC CAIO Council, determine the content of IC AI model registry entries.
- p. Establish and add to an IC AI risk management framework, including use restrictions and minimum risk management practices, in consultation with the IC CAIO Council.
- q. Receive and maintain a copy of IC element waivers to minimum risk management practices, and make those waivers available to the ODNI CLPO.
- r. Issue guidance on maintenance of inventories of IC element use cases and systems under AI use restriction and IC element waivers to minimum risk management practices.
- s. Coordinate IC guidance implementing section D.5.b. of this Directive that relates to civil liberties and privacy with the ODNI CLPO.
- t. Share notifications with the IC CAIO Council, as appropriate, of changes to IC element AI that could negatively affect another IC element's ability to conduct necessary business operations or degrade performance of an assigned IC function.
- u. Establish procedures, in consultation with the IC CAIO Council, to share information within the IC and with DoD, at a minimum when an AI system developed, deployed, or used by a contractor demonstrates risks related to safety, security, and trustworthiness, including to human rights, civil rights, civil liberties, or privacy. Specific procedures for when risks potentially affect U.S. person civil rights and liberties and privacy will be coordinated with the ODNI CLPO.
- v. Establish best practices or other guidelines, in consultation with the IC CAIO Council, on how to determine whether a given AI can reasonably reveal or recreate classified data to which it has been exposed.
- w. Work to align IC classification practices for AI and AI-derived outputs, and deconflict IC element determinations about whether a given AI has the reasonable potential to reveal or recreate classified data.
- x. Identify or develop AI-related competencies, knowledge, and skills for different roles within the IC with the IC HC.

2. IC element heads shall:

- a. Designate, in writing, their IC element CAIO, in coordination with the IC CAIO on behalf of the DNI. Designations shall be forwarded to the IC CAIO within 30 days of signature of this Directive, and thereafter within 15 days of new designations.
- b. Inform the IC CAIO about the progress, status, adoption, and management of AI within their IC element and the implementation of this Directive, in response to IC CAIO requests.
- c. Establish and implement procedures to report, as appropriate, misuse of AI internally to the IC element CAIO, to appropriate oversight offices, and externally to the IC CAIO, along with supporting procedures for response to such reports.

- d. Implement IC guidance on the use of AI trained or fine-tuned using data that potentially contained U.S. person information, publicly available information, commercially available information, or intellectual property.
- e. Implement IC guidance on the use of AI to analyze data that either includes U.S. person information as an input or that may produce U.S. person information as an AI output.
- f. Develop and apply safeguards to ensure IC element AI provides appropriate protection for civil liberties and privacy, including adherence to IC guidance on AI ethics and compliance with the Privacy Act.
- g. Perform impact assessments on IC element AI consistent with NSM-25 and the AI Framework.
- h. Oversee IC element AI throughout its lifecycle, through its disposition or removal from use.
- i. Establish and implement processes for identifying accountability for and responding to unexpected, inaccurate, or unintentionally biased IC element AI outputs.
- j. Periodically audit IC element AI.
- k. Document and register each IC element AI model on a model registry entry in the IC AI model registry.
- l. Identify, characterize, assess, and manage risk using the IC AI risk management framework.
- m. Issue waivers to minimum risk management practices, and report to the IC CAIO approvals and renewals of waivers to minimum risk management practices for AI use restrictions within 3 days of issuance.
- n. Maintain an inventory of IC element use cases and systems that fall under AI use restrictions as well as IC element approved waivers to minimum risk management practices consistent with guidance issued by the IC CAIO, and report the inventory and waivers to the IC CAIO upon request.
- o. Establish and implement a process to evaluate and approve proposals to use or reuse AI for their IC element's given use case.
- p. Preapprove the use of malicious techniques against IC element AI.
- q. Test and evaluate IC element AI to identify unexpected performance shifts.
- r. Notify the IC CAIO of unexpected, upcoming, imminent, or ongoing changes to IC element AI, which could significantly negatively affect another IC element's ability to conduct necessary business operations or could degrade performance of an assigned IC function.
- s. Ensure that IC element AI complies with all applicable data classification and handling requirements, including by assessing whether each AI has the reasonable potential to reveal or recreate classified data to which it has been exposed by an authorized recipient of that

intelligence, and by implementing processes to ensure IC element AI outputs are classified appropriately.

t. Implement processes to ensure IC element AI outputs are classified appropriately.

u. Ensure their workforce has the requisite foundational and, as appropriate, advanced AI-related competencies, knowledge, and skills.

3. The IC CIO shall:

a. Coordinate and collaborate with the IC CAIO to ensure the IC Information Environment enables implementation of AI and that proposed IC AI guidance is consistent with IC CIO guidance.

4. The IC CDO shall:

a. Coordinate and collaborate with the IC CAIO to ensure that data is managed and data tradecraft is implemented throughout the lifecycle of IC AI; and to ensure that proposed IC AI guidance is consistent with IC CDO guidance.

b. Coordinate on mitigating unintended bias issues with the IC CAIO.

c. Coordinate on IC guidance on the use of AI trained or fine-tuned using data that potentially contained U.S. person information, publicly available information, commercially available information, or intellectual property.

d. Coordinate on IC guidance on the use of AI to analyze data that either includes U.S. person information as an input or that may produce U.S. person data as an AI output.

e. Establish, in consultation with the IC CAIO and the IC CDO Council, minimum standards for the documentation of data used to train any model developed, procured, or used by or on behalf of an element of the IC. At a minimum, standards shall be established for documentation of imputed, augmented, or synthetic data used to train IC AI.

5. The ODNI CLPO shall:

a. Coordinate and collaborate with the IC CAIO to ensure that guidance issued under this Directive protects privacy and civil liberties; civil liberties, privacy, and transparency are appropriately incorporated into the AI-related procedures of IC elements, consistent with ICD 107; and IC AI activities related to civil liberties, privacy, and transparency are reported appropriately.

b. Coordinate on mitigating unintended bias issues with the IC CAIO.

c. Coordinate on IC guidance on the use of AI trained or fine-tuned using data that potentially contained U.S. person information, publicly available information, commercially available information, or intellectual property.

d. Coordinate on IC guidance on the use of AI to analyze data that either includes U.S. person information as an input or that may produce U.S. person information as an AI output.

e. Periodically submit a report to the DNI on activities associated with IC AI oversight.

f. Coordinate on IC guidance implementing section D.5.b. of this Directive that relates to civil liberties and privacy.


g. Coordinate on IC CAIO procedures to share information within the IC and with DoD about AI-related risks related to safety, security, and trustworthiness, including to human rights, civil rights, civil liberties, or privacy, at a minimum for AI developed, deployed, or used by a contractor, when those risks potentially affect U.S. person civil rights and liberties and privacy.

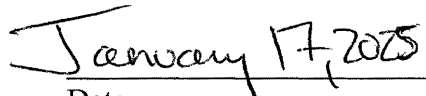
6. The Chief, IC DEIA shall:

a. Coordinate and collaborate with the IC CAIO to ensure compliance with relevant non-discrimination and accessibility laws and policy.

b. Coordinate on mitigating unintended bias issues with the IC CAIO.

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

  
\_\_\_\_\_  
Director of National Intelligence

  
\_\_\_\_\_  
Date