

Intelligence Community Data Management

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order 12333, as amended; and other applicable provisions of law.

B. PURPOSE

1. This Intelligence Community Directive (ICD) establishes policy for the standardization and governance of data that the Intelligence Community (IC) collects, acquires, creates, holds, stores, accesses, or uses to maximize and provide consistency in its usability and interoperability.

2. This ICD incorporates provisions from, and rescinds, ES 2017-00072, *Designation of Mr. Stephen D. Prosser as the IC Chief Data Officer and Role and Responsibilities of the IC Chief Data Officers*, 2 February 2017.

C. APPLICABILITY: 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.

D. POLICY

1. The IC must fully realize investments made in the collection, acquisition, and creation of data. By effectively managing data to maximize its usability and interoperability, and by leveraging technological innovations that make data interoperable, the IC will be able to bring its data together in new ways to deliver compelling insights at the speed of mission. To accomplish this, the IC shall establish and implement a common data governance construct and accompanying standardized data management framework.

a. Consistent with 44 U.S.C. Sec. 3502(16), data is recorded information, regardless of form or the media on which the data is recorded.

b. Data that an IC element holds or stores as a technical service to a non-IC partner, but which the IC element does not access or use in any way for its own intelligence purposes, is excluded from the scope of this Directive.

c. For the purpose of this Directive, the term “data” refers to any data collected, acquired, created, held, stored, accessed, and/or used by any element(s) of the IC (e.g., mission, business, operations, research, support, and administrative functions of the IC element).



2. The IC Chief Data Officer (CDO) shall oversee and set the strategic direction for IC data management.

3. IC element heads shall designate a CDO for their IC element who is responsible for providing leadership, strategic direction, and oversight of IC element data and its governance in accordance with Office of the Director of National Intelligence (ODNI) guidance. In IC elements with a statutory CDO, the statutory CDO may serve as the IC element CDO. IC element heads shall submit to the IC CDO, in writing, the designation of their IC element CDO within 30 days of signature of this Directive, and thereafter within 15 days of new designations. IC element CDOs should be senior officials who shall possess:

a. Authority to speak on behalf of their element with regard to, as well as make decisions about, developing, implementing, and overseeing data governance and data management for data held by their element, consistent with the provisions of this Directive;

b. Skills, knowledge, and expertise necessary to span the IC element's enterprise business and mission needs and the capabilities of its information technology; and

c. Insight into all data collected, acquired, created, held, stored, accessed, or used by their IC element sufficient to execute the provisions of this Directive.

4. The IC Chief Data Officer Council (IC CDOC) shall be chaired by the IC CDO, be comprised of IC element CDOs, and be focused on the strategic direction of IC data governance. The IC CDOC shall serve as a source of data management advice for the IC CDO and provide a forum for members to share best practices.

5. Upon request, IC element CDOs shall inform the IC CDO about the management of data and the implementation of this Directive.

6. IC elements shall automate data management activities, including those that enable discovery of, access to, and sharing of data. All automated data management activities shall comport with legal and policy requirements.

7. The IC CDO shall establish an IC data management planning framework that includes the collecting, acquiring, creating, processing, disseminating, using, storing, and disposing of data. This framework shall include provisions to enable implementation of relevant data security and data protection requirements.

8. IC elements shall, for data collected, acquired, created, held, and/or stored by their element:

a. Implement the IC's data management planning framework, including provisions to enable implementation of relevant data security and data protection requirements;

b. Plan for data management needs before collecting, acquiring, creating, holding, and/or storing data;

c. Document, via data management plans, the management of data throughout its lifecycle. For unanticipated data collection, data management should be planned and documented as soon as practical, and no later than 30 days post collection;

d. Plan for, document, and ensure compliance with legal and policy requirements for data management. At a minimum, this shall include:

(1) Adherence to policy requirements related to civil liberties, privacy protections, and transparency considerations in accordance with ICD 107, *Civil Liberties, Privacy, and Transparency*.

(2) Protection relating to the collection, retention, and dissemination of U.S. Persons data, in accordance with Executive Order 12333 and applicable Attorney General guidelines and other applicable laws and policy.

e. Designate accountable data management professionals responsible for managing data throughout its lifecycle.

9. IC elements shall ensure all data collected, acquired, created, held, stored, accessed, and/or used by their IC element is inventoried and is described and cataloged in the IC Data Catalog provided by the IC Data Services Service of Common Concern (SoCC). For data exempt from discovery under IC Policy Guidance (ICPG) 501.1, *Exemption of Information From Discovery*, IC elements may fulfill this requirement via a separate inventory, description, and catalog.

10. The IC CDO, in consultation with the IC CDOC, shall establish common data tags to describe and manage data. The IC Chief Information Officer (CIO) shall be consulted to ensure IC systems and architecture can support those common data tags. Upon establishment of common data tags, IC elements shall apply those common data tags to:

- a. All electronic data that their IC element collects, acquires, and/or creates thereafter;
- b. All electronic data added to IC element holdings and/or storage thereafter; and
- c. All legacy electronic data, to the extent practicable.

11. Electronic data shall be managed to:

- a. Enable discoverability, accessibility, usability, and auditability for humans, technology, and analytic capabilities;
- b. Enable availability and interoperability within and across security domains, consistent with classification and handling restrictions;
- c. Serve both current and future needs; and
- d. Implement contractual and security requirements.

12. IC elements shall ensure that data management plans include acquisition or access agreements and arrangements, to enable effective data management throughout its lifecycle, consistent with the provisions of this Directive.

13. Electronic data that IC elements collect, acquire, create, hold, and/or store shall be structured and managed to maximize the IC's ability to receive data from, transmit data to, and share data with external mission partners and stakeholders, including the Department of Defense; other U.S. Government departments and agencies; state, local, tribal, and territorial governments; foreign partners; and the private sector, while maintaining data utility and conformance with legal, policy, and compliance requirements.

14. IC elements shall adhere to relevant guidance and frameworks on ethical data management, including the *Artificial Intelligence Ethics Framework for the Intelligence Community* or successor framework.

15. IC elements shall use IC Data Services designated as SoCC. Exceptions will conform to the requirements established in ICD 121, *Managing the IC Information Environment*.

16. The IC CDO, in consultation with IC Human Capital (HC), shall develop or identify criteria and training material for foundational and advanced data management knowledge and skills. IC element heads shall ensure their workforce has the requisite foundational and, as appropriate, advanced data management knowledge and skills. IC elements may accomplish this through training material identified or developed by the IC CDO, or through other training material that incorporates content meeting the criteria established by the IC CDO.

E. ROLES AND RESPONSIBILITIES

1. The IC CDO shall:

- a. Advise the DNI on matters related to data management.
- 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 for IC data governance and IC data management.
- e. Maintain a record of designated IC element CDOs.
- f. Serve as Chair of the IC CDOC.
- g. As needed, solicit input from IC element CDOs about the management of data and the implementation of this Directive.
- h. Establish an IC data management planning framework that includes the collecting, acquiring, creating, processing, disseminating, using, storing, and disposing of data, as well as provisions to enable implementation of relevant data security and data protection requirements.

- i. Establish data tags in coordination with the IC CDOC.
 - j. Consult with the IC CIO to ensure IC systems and architecture can support common data tags.
 - k. Ensure incorporation of legal rights and policy requirements for civil liberties, privacy, and transparency into data management oversight activities.
 - l. Ensure IC data management oversight incorporates relevant ethics guidance.
 - m. Identify or develop criteria and training material for foundational and advanced data management knowledge and skills, in consultation with the IC HC.
2. The IC CIO shall advise the IC CDO about whether IC systems and architecture can support common data tags.
 3. IC element heads shall:
 - a. Designate in writing IC element CDOs. Designations shall be forwarded to the IC CDO within 30 days of signature of this Directive, and thereafter within 15 days of new designations.
 - b. Upon request, inform the IC CDO about IC element data-related matters, including the strategic direction for IC element data governance and IC element data management; IC-level data-related matters affecting their IC element; and the implementation of this Directive within their IC element.
 - c. Automate data management activities, including those that enable discoverability, access, and sharing of data. All automated data management activities shall comport with legal and policy requirements.
 - d. Establish data management roles and implement the IC's data management planning framework, including provisions to enable implementation of relevant data security and data protection requirements.
 - e. For data collected, acquired, created, held, and/or stored by their element, plan for data management needs; document, via data management plans, the management of data throughout its lifecycle; plan and document compliance with applicable legal and policy requirements for data management; and designate accountable data management professionals responsible for managing data throughout its lifecycle.
 - f. Ensure all data collected, acquired, created, held, stored, accessed, and/or used by their IC element is inventoried and is described in the IC Data Catalog provided by the IC Data Services SoCC. For data exempt from discovery under ICPG 501.1 this requirement may be fulfilled via a separate inventory, description, and catalog.
 - g. For electronic IC data, apply common data tags developed in accordance with this Directive to all data that their IC element collects, acquires, creates, holds, and/or stores.

h. Ensure that data management plans include acquisition or access agreements and arrangements, consistent with provisions of this Directive.

i. Ensure legal rights and policy requirements for civil liberties, privacy protections, and transparency are incorporated into IC element data management activities.

j. Ensure ethics considerations are incorporated into IC element data management activities.

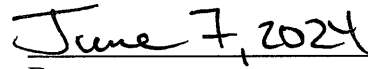
k. Use IC Data Services designated as SoCC, unless an exception conforms to the requirements established in ICD 121, *Managing the IC Information Environment*.

l. Ensure all IC personnel at their element possess foundational and, as appropriate, advanced data management knowledge and skills consistent with criteria established under this Directive.

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



Director of National Intelligence



Date