The IC OSINT Strategy 2024-2026

The INT of First Resort: Unlocking the Value of OSINT

UNITED STATES INTELLIGENCE COMMUNITY
COLLABORATUS
VIRTUS
FIDES

Table of Contents

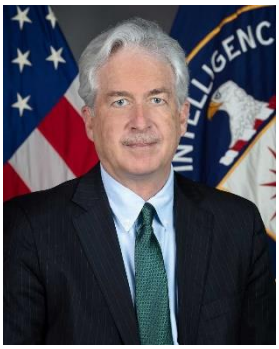
From the Director of National Intelligence ..... **i**
From the IC OSINT Functional Manager ..... **i**
IC OSINT Strategy 2024-2026 ..... **1**
Introduction **2**
Strategic Focus Areas **3**
Key Enablers **6**
Way Forward **6**

From the Director of National Intelligence

By harnessing the potential of Open Source Intelligence (OSINT), the Intelligence Community (IC) will continue to provide comprehensive support to national security policymakers and will create additional opportunities to be transparent with our partners and the public about the threats we face. To achieve this desired outcome, we must establish a common vision and firm foundation that are consistent with the values of free and open societies. The IC OSINT Strategy represents the beginning of a long-term process that will professionalize the OSINT discipline, transform intelligence analysis and production, and create new avenues for partnering with brilliant American innovators and like-minded foreign partners.

Avril D. Haines

From the OSINT Functional Manager



As the IC's Functional Manager for OSINT, I know the critical role that OSINT plays in defending our country and values. From operations and analysis, to policy meetings, OSINT informs the decisions of senior policymakers on nearly every major issue facing the United States. In this pivotal moment, when OSINT is increasingly important and growing in demand, an IC-wide OSINT strategy is key to helping the IC move forward in a coordinated and determined way. This strategy will help us fulfil our responsibilities and increase the already-tremendous impact that the OSINT discipline is having on the safety and security of our nation.

William J. Burns, D/CIA

IC OSINT Strategy 2024-2026

OSINT Definition: OSINT is intelligence derived exclusively from publicly or commercially available information that addresses specific intelligence priorities, requirements, or gaps.

Mission	Vision
IC professionals collect, create, and deliver timely, relevant, and insightful open source intelligence to inform national security decisions and protect our Nation and its interests.	A professionalized, integrated, and agile IC OSINT enterprise providing decision advantage for U.S. policymakers and warfighters and driving innovation with partners.

Strategic Focus Areas

This IC OSINT Strategy comprises four strategic focus areas that, taken together, will strengthen OSINT as a core intelligence discipline and position the IC to capitalize on the full potential of open source data and information to enhance the intelligence mission in a manner consistent with our nation's principles and values.

- Coordinate Open Source Data Acquisition and Expand Sharing
- Establish Integrated Open Source Collection Management
- Drive OSINT Innovation To Deliver New Capabilities
- Develop the Next-Generation OSINT Workforce and Tradecraft

In addition to the four focus areas, this strategy recognizes that effective and supportive governance and robust partnerships with industry, academia, and foreign counterparts will be essential for success in the OSINT mission and key enablers of the IC OSINT Strategy. The OSINT Functional Manager, in partnership with the IC OSINT Executive and the Defense Intelligence Enterprise Manager for OSINT, will lead implementation of this strategy, including identifying concrete actions the IC will take to achieve the strategy's objectives and measure outcomes. Given the fast pace of change in the open source environment, the OSINT Community will review the strategy on an annual basis and develop an iterative action plan each year to guide implementation efforts.

Introduction

OSINT is vital to the Intelligence Community's Mission. OSINT both enables other intelligence collection disciplines and delivers unique intelligence value of its own, allowing the IC to more efficiently and effectively leverage its exquisite collection capabilities. As the open source environment continues to expand and evolve at breakneck speed, the ability to extract actionable insights from vast amounts of open source data will only increase in importance.

Rapid advances in artificial intelligence and machine learning present significant opportunities to capitalize on the value of OSINT. At the same time, the IC must be attuned to the risks in the open source domain, including the provenance and validity of information it obtains. To maintain an intelligence advantage in the open source environment, we must embrace new technologies and tradecraft to collect and evaluate open source data. At the same time, the IC must reimagine its relationships with industry and academia to leverage cutting-edge capabilities being developed and applied in the private sector. Because of the unclassified nature of open source information, OSINT presents a unique opportunity among collection disciplines to explore new partnership models to speed the adoption of new tools and tradecraft.

For the IC to surpass nation-state competitors that are making significant investments in the open source domain, we must build an integrated and agile OSINT community that can rapidly innovate as the open source environment evolves. The IC OSINT Strategy provides the framework for integrating OSINT more fully into IC workflows, tradecraft, and all-source analysis, while ensuring appropriate protections for privacy and civil liberties. To advance the OSINT discipline, the IC will streamline data acquisition, develop innovative technologies to collect and derive insight from open source data, strengthen the coordination of open source collection activities across the community, update and standardize OSINT tradecraft, and develop a highly skilled OSINT workforce. Through these efforts, we will work together to leverage the full power of OSINT to support IC analysts and operators and ensure the IC is poised to provide decision advantage for warfighters and national security policymakers.

Strategic Focus Areas

Goal: Coordinate Open Source Data Acquisition and Expand Data Sharing

Coordinate the acquisition of open source data to avoid redundancy and expand data sharing, as appropriate, to enable mission and ensure the most efficient use of IC resources.

All members of the IC should be able to discover IC-acquired open source data and community OSINT reporting, while adhering to security and classification requirements. Expanding the accessibility of Publicly Available Information (PAI) and Commercially Available Information (CAI) will maximize the return on IC investment and increase the value of open source data and tools across all IC missions.

To ensure the most efficient acquisition models and broadest possible sharing of data across the community, OSINT leaders will partner with IC Data Officers and others to coordinate the distributed acquisition of PAI and CAI, with consideration for its ethical and appropriate use, consistent with law and policy. These processes will consider the value and necessity of the data for IC mission uses, as well as the equities of multi-mission departments and agencies when acquiring data for both intelligence and non-intelligence purposes. The IC will regularly review usage metrics and mission impact for all data purchases to ensure the best use of IC resources.

In accordance with the Director of National Intelligence's (DNI) direction, the IC will implement the CAI Framework and track PAI and CAI in a centralized, multi-domain data catalog to enhance transparency. The OSINT community will leverage ongoing efforts to enhance data management across the IC through the development of interoperability and data tagging standards to ensure data reaches mission users in a timely and usable manner. In addition, the IC will establish common OSINT platforms to facilitate access to shared data and tools, and we will identify and implement a pathway to deliver IC OSINT products to the broader U.S. Government.

Goal: Establish Integrated Open Source Collection Management

Align and manage open source collection efforts across the IC to enhance the speed and awareness of collection while avoiding duplication of effort.

Integrated collection management is a foundational necessity to ensure that the IC's open source collection efforts are optimized to meet varied and evolving national security and IC mission requirements. The OSINT enterprise must develop agile processes and workflows to coordinate collection activities across the IC, make adjustments as needed, and ensure compliance with privacy and civil liberties protections. These processes and workflows must be grounded in a common baseline of open source collection activities that includes a gap analysis against priority collection requirements and the identification of IC elements best postured to address critical gaps.

Going forward, IC open source collection efforts will require sustained coordination and deconfliction through existing OSINT governing bodies. This deconfliction is necessary both within the OSINT community and across intelligence collection disciplines to ensure that the IC is not expending its most sensitive collection capabilities to obtain intelligence that can be derived from open source information.

To further professionalize OSINT as a discipline and ensure the speed and agility of OSINT collection management, the IC must establish a new and improved community-wide collection orchestration system that enables collective visibility on requirements and collection efforts. Such a system will also enable the collection and evaluation of metrics that are critical for the planning and evaluation of collection operations to ensure OSINT resources are delivering mission impact.

Goal: Drive OSINT Innovation To Deliver New Capabilities

Develop and adopt sophisticated tools to exploit open source data and information.

The rapid expansion of open source data and platforms requires the IC to constantly adapt its tools and tradecraft to sustain the ability to deliver timely and credible open source information to policymakers and warfighters at speed and scale, and in a range of formats tailored to various mission and consumer requirements. The OSINT community is already pioneering new uses of artificial intelligence, machine learning, and human language technologies for the OSINT mission. The IC must expand and accelerate these efforts to sustain a competitive edge. Speed of innovation will be a critical measure of success, and the IC must embrace the ability to test new capabilities on unclassified systems that present fewer risks and barriers than classified networks.

External partnerships will be vital to success in this domain. The IC must be postured to capitalize on pioneering efforts in the private sector by partnering in new ways with industry and academia to develop, test, and deploy OSINT tools and tradecraft.

Goal: Develop the Next-Generation OSINT Workforce and Tradecraft

Establish and evolve common OSINT tradecraft standards and an IC workforce capable of identifying, extracting, and delivering insights from open source data and information in the dynamic open source technology landscape.

The IC requires common OSINT tradecraft and training standards that are compatible with other intelligence discipline tradecraft and training standards to ensure all OSINT activities are conducted in a manner that protects IC collection requirements and sources, and safeguards U.S. persons' information and privacy. Tradecraft and training standards must be flexible and updated regularly to keep pace with changes in the open source domain.

The growth of generative artificial intelligence (GAI) presents both opportunities and risks for OSINT tradecraft. GAI can be a powerful tool to enable timely and insightful OSINT production, including by aiding the identification of common themes or patterns in underlying data and

quickly summarizing large amounts of text. At the same time, OSINT tradecraft and training must be updated and refined to mitigate the potential risks of GAI, including inaccuracies and hallucinations. The OSINT community should be at the forefront of the IC in testing the use of GAI and developing and evolving the tradecraft for its use. This tradecraft will set the standards for the human-machine teaming that will be the foundation of OSINT in the future.

Dynamic training is core to developing a cadre of IC professionals who have the skills and expertise to keep pace with the rapidly evolving digital environment and open source landscape. The IC must develop clear training pathways with skill expectations from the foundational to the expert level, to include data acumen and technical aptitude. At the same time, the OSINT discipline will continue to require officers with the substantive, language, and cultural knowledge necessary to identify, collect, and exploit the best source of information to address priority intelligence requirements. OSINT tradecraft and training must address the needs of both OSINT professionals and all-source analysts who conduct OSINT activities. An IC workforce with expert open source skills is critical to the IC's ability to produce timely and accurate intelligence for national security decisionmakers.

Key Enablers

Governance

The strength of the IC OSINT enterprise is its federated approach, with participation and input from all 18 IC organizations. At the same time, the wide range of OSINT activities and requirements across the IC increases the importance of effective and supportive governance to ensure coordination across the enterprise, establish standards, harmonize existing policies, and facilitate the development of new capabilities to address enterprise-wide challenges.

The Director of the Central Intelligence Agency (D/CIA) serves as the OSINT Functional Manager (OSFM) for the IC and delegates day-to-day functional management responsibilities to the Director of the Open Source Enterprise (D/OSE) to oversee and guide open source activities across the IC. CIA, as the Open Source Functional Manager[1], works in close collaboration with the Defense Intelligence Enterprise Manager for OSINT at the Defense Intelligence Agency (DIA) and the IC OSINT Executive at the Office of the Director of National Intelligence to develop IC policy and coordinate resource requests. The OSINT Executive also supports the implementation of the OSINT Strategy by establishing defined roles and responsibilities for IC elements as part of a federated OSINT enterprise, and ensuring alignment between the IC's and Department of Defense's open source activities.

Partnerships

The IC OSINT Strategy requires us to engage differently with academia, the private sector, and foreign counterparts. We must cultivate and deepen relationships with outside experts to keep pace with technical and tradecraft advancements in the open source environment. We must grow our relationships with foreign partners and establish durable agreements to share collection, tools, and tradecraft. Finally, we must commit to partnering differently within the IC OSINT Community by sharing new technologies, data, and insights acquired from sources external to the U.S. Government.

Way Forward

In order to evolve OSINT, the IC must work together with key partners to put into place the governance, partnerships, tradecraft, training, tools, data sharing, and collection best practices to achieve this strategy. The IC will develop an overarching *OSINT Strategy Action Plan* to identify discrete activities and milestones, develop metrics, and track results.

[1] Within the IC, the designated Functional Managers for their respective intelligence disciplines (commonly referred to as "INTs") are D/CIA for Human Intelligence (HUMINT) and OSINT; Director, National Geospatial-Intelligence Agency for Geospatial Intelligence (GEOINT); Director, Defense Intelligence Agency for Measurement and Signatures Intelligence (MASINT); and Director, National Security Agency for Signals Intelligence (SIGINT). The Functional Managers for HUMINT, GEOINT, and SIGINT were designated by Executive Order (EO) 12333. The Functional Managers for OSINT and MASINT were designated by the Director of National Intelligence, who was granted the authority to establish additional Functional Managers by EO 12333.

United States Intelligence Community

IC OSINT Strategy
2024-2026