



**Intelligence Community  
Information Environment (IC IE)  
Data Strategy**

**2017-2021**



# TABLE OF CONTENTS

ii	<b>MESSAGE FROM THE DNI</b>
iii	<b>MESSAGE FROM THE IC CDO AND IC ISSE</b>
i	<b>INTRODUCTION</b>
2	<b>VISION, MISSION, OPERATING PRINCIPLES</b>
3	<b>STRATEGIC GOALS</b>
4	<b>Goal 1: Develop and Institutionalize a Strategic Data Framework Across the Multi-fabric IC Information Environment</b>
6	<b>Goal 2: Ensure Data is Appropriately Protected, Shared, and Handled Across All Fabrics</b>
7	<b>Goal 3: Create, Resource, and Leverage Secured, Scalable and Shared Data Services that Meet the IC's Needs for Variety, Velocity, Volume, and Veracity</b>
8	<b>Goal 4: Champion a Culture that Encourages and Rewards Data-Centric Behaviors that Effectively Balance Sharing and Safeguarding</b>
ii	<b>THE WAY AHEAD FOR STRATEGIC IMPLEMENTATION</b>

## MESSAGE FROM THE DNI

Our nation faces an ever-evolving, increasingly complex, and diverse set of threats. The Intelligence Community (IC) is charged with the responsibility of providing the most timely, accurate, and insightful intelligence to counter these threats. For us to fulfill this role, we must bring all of the information possible to bear in producing high-quality intelligence upon which our customers depend. Rapid advances in technology have led to an explosion in the volume, velocity, and variety of data, and we must find innovative ways to exploit and establish relevance and ensure the veracity of our information.

The IC has made significant investments in an infrastructure that will allow us to integrate intelligence by sharing IC data and applying advanced analytic tradecraft and big data techniques. This infrastructure is largely built. Our job now is to prepare our data for use in the most effective way. We have traditionally managed data in silos and coupled it with IT solutions that store, process, exploit, and manage it. This has allowed us to build highly-tuned capabilities that work well for a specific data set or a specific mission need. However, given the explosive growth in our data, we must adapt our approach in a way that provides the utmost flexibility and better harnesses the power of data for our Community.

At the same time, we must implement safeguards to protect our sources and methods, and execute our national security mission in a way that protects civil liberties and privacy rights. Our policy framework enables us to perform the mission of intelligence while simultaneously maintaining those safeguards. The IC Chief Data Officer (CDO) and the IC Information Sharing and Safeguarding Executive (ISSE) are working collaboratively to identify impediments to information sharing, and develop solutions to safeguard data while enhancing intelligence integration. This Data Strategy provides the framework to address strategic issues that affect our ability to collect, analyze, produce, and disseminate intelligence relevant to the national security of the United States.



Daniel R. Coats  
Director of National Intelligence

## MESSAGE FROM THE IC CDO AND IC ISSE

In today's "big data" world, the Intelligence Community is acquiring, collecting, creating, and disposing of more data<sup>1</sup> than ever. For this information to be useful, we must rely less on our historic approach of using bilateral sharing agreements that constrain its use along organizational boundaries, and more on leveraging data services as the means to enforce all data handling and usage requirements for authorized IC personnel. We must no longer replicate data for different missions or disparate systems constrained by individual programs of record, but take advantage of our big data platforms to leverage all data that will help us gain insights.

This strategy describes a new approach to managing *Data as an IC Asset* – that is, maximizing use of data that may be relevant to one or more IC element for intelligence purposes. Interdisciplinary use of the IC's vast collection of intelligence information is critical to produce timely, accurate, thorough, and integrated intelligence positions. To do this, we will "free the data" by removing its current dependencies on IC element applications, systems, and databases, thus allowing it to be cataloged, self-described, and discoverable by automated means. Just as important, we will ensure that we apply safeguards and applicable legal and policy requirements for handling, use, and dissemination consistently across the enterprise.

This strategy document describes the overarching vision, mission, and objectives to make the *right data* available to the *right people*, at the *right time* and, in the *right form* to enable data- and analytic-driven decisions for our intelligence mission. This IC Information Environment (IC IE)<sup>2</sup> Data Strategy is grounded in public and private sector best practices and the principles presented by IC Directive (ICD) 501, *Discovery and Dissemination or Retrieval of Information within the IC*; ICD 121, *Managing the IC Information Environment*; and the National Intelligence Strategy. The goals and objectives described in the strategy will be used to guide the creation of implementation plans.

The IC CDO and the IC ISSE partner with IC elements to realize an IC-wide strategic direction is set forth for IC enterprise data and information sharing. Through the IC CDO Council and the Information Sharing Steering Committee, we will oversee and prioritize implementation of the principles described in this IC IE Data Strategy.



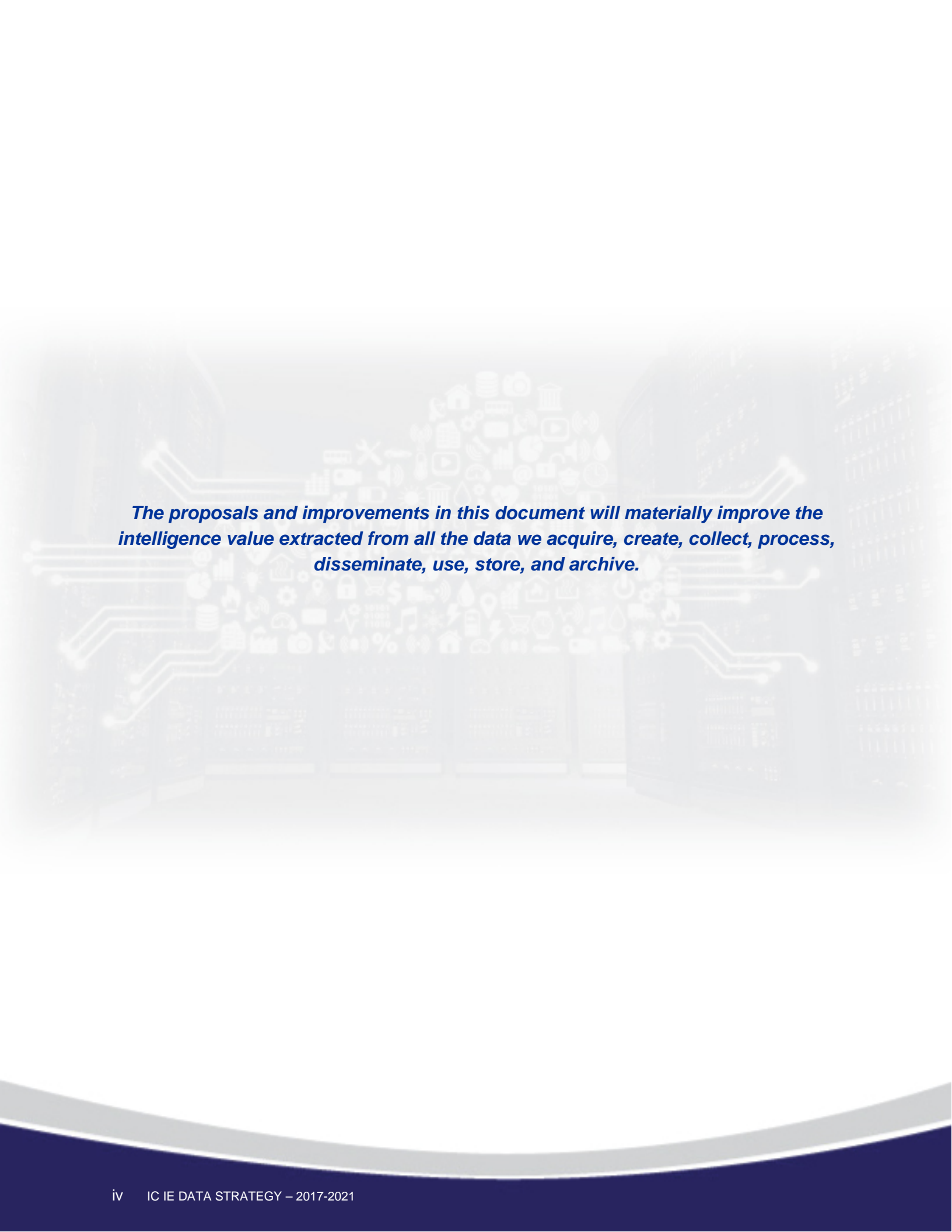
Stephen D. Prosser  
Intelligence Community Chief Data Officer



James A. Smith  
Intelligence Community Information  
Sharing and Safeguarding Executive

<sup>1</sup> Within this document, the term, "data" means data and information categorized as either mission or business.

<sup>2</sup> Within this document, the IC IE refers to individuals, organizations and Information Technology capabilities that collect, process or share Sensitive Compartmented Information, or that, regardless of classification, are operated by the IC.



***The proposals and improvements in this document will materially improve the intelligence value extracted from all the data we acquire, create, collect, process, disseminate, use, store, and archive.***

## INTRODUCTION

Informed decisions based on accurate, timely, insightful, and objective analysis are critical to provide the front-line of defense against threats to the U.S. and its global partners. The IC is a critical component of the national security structure that provides the information necessary to address those threats. The intent of this *IC IE Data Strategy* is to guide the IC toward a common, more secure, and more integrated enterprise by leveraging the vision and framework of the IC IE to operationalize a data-centric community. The Strategy sets out goals and objectives for data-centricity that call upon IC elements to place mission and business data at the center of every plan to drive mission success.

The goal of the *IC IE Data Strategy* is to ensure the *right data* gets to the *right people* at the *right time* in the *right form*. Today's challenges require new approaches to IC operations and mission support. Our nation continues to confront challenges posed by globalization, the blurring of foreign and domestic threats, and demand for speed-of-decision required by the overlap of intelligence and operations. Evolving cyber threats have also focused attention on the need to protect personal identifiable information, regardless of source, from unauthorized users. The challenges of delivering data must be addressed in a dynamic environment characterized by differing approaches to both formal and informal interagency collaboration, and different authorities to acquire, collect, curate, retain, and share data. These processes operate against a backdrop of unabated growth in information. A majority of IC data is also tightly coupled with the data management and mission-analytic capabilities of IC element-specific systems. Ultimately, achieving data-centricity will require separation of the data from these applications.

ICD 501 directs that IC elements have the "responsibility to provide" and authorized IC personnel have the "responsibility to discover and request" data that can contribute to their assigned mission. This sharing imperative also applies to law enforcement, the rest of government, and our international partners. To instill these disciplines in the IC, we must foster a culture where our people maximize the value of data across the IC, and have the tools and abilities to effectively use it. In a data-driven culture, data is the concern of every employee, not just data architects, scientists, and providers; it further requires placing data sharing at the center of all forms of decision-making.

Expanding the overall value of IC data that may be relevant to one or more IC elements for intelligence purposes requires a common operating model that describes and incentivizes the adoption of rules for acquisition, sharing, discovery, access, and use. A secure, fully data-centric environment will separate data from applications, and make data available to a broad range of tools and analytics within and across security domains for enrichment and discovery. The environment must embrace a more disciplined approach to intelligence integration by ensuring that data is sharable, discoverable, accessible, retrievable, and protected. Finally, the IC needs to evolve its governance process to manage policy, standards, and prioritization of shared data management resources. Rather than individual sharing agreements, IC elements should utilize multilateral arrangements where appropriate, and rely more on data services as a means to enforce all of the legal and policy requirements governing access, use, dissemination, or retention of information.

Intelligence integration is more important than ever, and establishing an IC framework for realizing the principle of *Data as an IC Asset* will enable a full range of data and mission uses.

## VISION:

*The right data to the right people  
at the right time.*

## MISSION:

*Make IC data discoverable, accessible,  
and usable at the speed of mission.*

## OPERATING PRINCIPLES:

### **Mission First**

Make decisions based on intelligence mission needs.

### **Leadership**

Provide strategic leadership across the IC.

### **Partnership**

Achieve unity of effort through teamwork, collaboration, and transparency.

### **Innovation**

Leverage technology to increase effectiveness and drive efficiency.

### **Achievement**

Deliver an integrated, secure enterprise to satisfy the highest mission priorities.



# 1

### **Develop and institutionalize a strategic data framework across the multi-fabric IC Information Environment**

Free data so it can be discovered, accessed, linked, and used independently by mission applications and common IC services. Align and strengthen policies and practices toward a shared vision to leverage Community investments to increase standardization, efficiency and interoperability.

# 2

### **Ensure data is appropriately protected, shared, and handled across all fabrics**

Promote a common approach for security and privacy that advances secure, cross domain sharing of data.

# 3

### **Create and resource scalable shared data services that meet the IC's needs for variety, velocity, volume, and veracity**

Provide leadership on strategic needs for shared data services throughout the data life cycle. Develop integrated governance and management processes that promote standards-based services that are technical enablers for new and innovative methods for using data to accelerate the pace and quality of analytic insight. Free our data scientists to do data science, not data wrangling.

# 4

### **Foster a culture that champions, encourages, and rewards data-centric behaviors that effectively balance sharing and safeguarding**

Advocate for information sharing across the IC and reduce unnecessary barriers that impede discovery, access, trust, and usability. Promote effective data stewardship by shaping education, awareness, training, and development to reinforce data-centric behavior. Strengthen and leverage industry, academia, and government partnerships to accelerate innovation in tradecraft to meet mission needs.

# STRATEGIC GOAL 1

## Develop and institutionalize a Strategic Data Framework across the multi-fabric IC Information Environment

The reliance of IC element analysts and users on incomplete or constrained sets of data precludes the discovery of contrary, supportive, or enhanced information held by others. This limits fully-informed analysis and decision-making. Historically, IC elements have protected their data by isolating it in silos, and managing it for IC element-specific missions. Freed data can be discovered, accessed, linked, and used independently by mission applications and common IC services that leverage multiple databases and analytic environments. Removing unnecessary barriers to sharing will allow the IC to realize the full potential of the data it acquires, collects, or creates. As the data applied to intelligence problems continues to increase in volume, variety, and velocity, the IC has a tremendous opportunity to improve the scope and scale of discoverability to enable greater information sharing that leads to intelligence insights. Engaging with stakeholders, to include collectors, analysts, data scientists, and IT professionals, will allow the Community to understand its challenges. Engagement also allows the IC to develop processes, standards, and techniques to integrate diverse sources of data that can have unique handling, safeguarding, and intelligence oversight needs.

### OBJECTIVES:

#### Establish a common reference data architecture

Develop and reach Community agreement on a data architecture that provides detailed architectural information in compatible formats to enable solutions to be repeatedly designed and deployed in a consistent, high-quality, and supportable fashion. The architecture will establish standards that are scalable and agile, built on the concept of data-centricity to facilitate extraction of data in multiple formats, and apply to a range of uses as internal and external needs change.

#### Create a common data management lexicon

Connect the language of data management across the IC through agreed-upon understanding of the terms and definitions for data management. Encourage the use of best practices and widely-used industry standards to improve the fidelity of terminology so that activities inherent to, and supporting, the IC can communicate effectively.

#### Develop ontology strategy

The diversity of data sources used by the IC creates a challenge to the process of managing or aggregating data. Adopting consistent ontologies mitigates this challenge by providing a mechanism to enhance the available descriptions for IC data assets into domains or subject

areas. The IC will develop an ontology strategy that includes goals, evaluation criteria, processes, and success factors to achieve greater mission effectiveness from combined data. The IC ontology strategy will guide formal naming conventions and the definition of common data types, properties, and interrelationships, which will serve as the basis for processing IC data for integration. Resulting outcomes will balance fidelity, accuracy, and completeness against practical constraints and resources.

### **Leverage and enhance common standards to enable discovery, access, and use of data**

Champion efforts across the IC to achieve an agreed-upon, interoperable, comprehensive data-tagging methodology that complies with IC standards for core data-management functions, and can be tailored to mission-specific uses. Incorporated data tagging and metadata standards are essential to data interoperability.

### **Align IC policies and practices with the IC IE Data Strategy**

Ensure the tenets laid out in this data strategy are incorporated consistently into new or modified policies and practices. Govern and manage IC enterprise data, and evaluate IC element policies, procedures, and practices needed to achieve success. Standardize policies, procedures, and practices to the extent possible, consistent with the foundation formed by the common data management lexicon. The IC should also provide maximum transparency and coordination with relevant oversight bodies regarding the collection and use of data.

### **Map data management rules to authorities and policies and ensure the rules are machine-executable**

Agree on and synchronize a core set of data management rules or standards among IC elements. This core set would establish a foundation to automate effective capabilities and business processes that control and protect data in accordance with all relevant authorities and policies.

### **Ensure the achievement of mandated IC-wide sharing objectives through the adoption of multilateral agreements in place of bilateral sharing arrangements**

Replace historical reliance on bilateral data sharing agreements with more transparent, reliable, replicable, and manageable multilateral agreements to support sharing among IC elements, and between elements and Non-Title 50 Agencies. For acquired data, implement the principles described in ODNI Executive Correspondence 2017-00342, *Guiding Principles to Enable IC Sharing of Acquired Data*.

# STRATEGIC GOAL 2

## Ensure data is appropriately protected, shared, and handled across all fabrics

Data should be available to any IC employee who is cleared for access and has an appropriate need-to-know, and enable the IC employee to assess if the information is of possible relevance to their assigned mission. At the same time, data must be safeguarded, sources and methods protected, and the civil liberties and privacy of U.S. persons respected. As appropriate, the IC will identify and mitigate technical, operational, and policy barriers to data access for those who support and conduct IC missions. The IC will promote policies and practices that enhance cross domain discovery and attribute-based access controls for both individuals and non-person entities, with a consistent focus on both information sharing and protection. Effective intelligence support for the nation's security requires a resilient, documented, and scalable foundation comprised of shared best practices, common standards, and innovative technologies.

### OBJECTIVES:

#### Establish and guide secure data access across multiple security fabrics

Ensure a common understanding and implementation of access control rules, including use, policy, and safeguards. Better resolve mission challenges with data discovery and access by making more informed decisions that consider both mission needs and information protection concerns. Provide guidance for the authority, classification, and use of data and information that is integrated, aggregated, compiled, or fused.

#### Advocate common access control and auditing frameworks

Resolve present bilateral and multilateral sharing impediments based on differences in auditing requirements and controls. Automate controls that establish a common approach for access and handling controls for authorized users to protect confidentiality, integrity, and availability. The ODNI will collaborate with IC elements to build a durable framework for use, policy, and security that can be applied uniformly.

#### Drive adoption and integration of a common attribute architecture

IC elements will work through the Identification, Authentication, and Authorization (IAA) Program Office and attribute providers (entitlement management, etc.) to drive common adoption for a given security fabric and consistent integration across security fabrics.

#### Champion the development and adoption of an IC data risk mitigation approach

Adopt a common data risk mitigation framework to identify and help manage areas of risk throughout the complete data life cycle. An approach to associating risk and safeguarding requirements to specific types of intelligence information will be critical to ensure the IC IE provides the desired automation to benefit mission.

## **Create and resource scalable shared data services that meet the IC's needs for variety, velocity, and volume**

Data services are critical to ensuring access to data for appropriate use, wherever it is located. Data services must mature in order to provide services such as ingesting, conditioning, cataloging, and indexing to maximize sharing and appropriate use of capabilities. The IC will provide an interoperable set of end-to-end data services to maximize efficiency and utility for data consumers. IC elements should rely more on data services as a means to enforce all of the legal and policy requirements governing access, use, dissemination, or retention of information.

### **OBJECTIVES:**

#### **Drive the implementation of shared data services and supporting governance**

Direct the development and implementation of IC IE core data services that enable full life cycle management to meet data provider and consumer needs. Provide guidance for critical, strategic data capabilities to promote, manage, expose, and sustain interoperable, platform-independent enterprise services. Establish an integrated governance process to identify and prioritize data service requirements gathered from the Community. Ensure services adhere to IC data standards of consistency, interoperability, and maximum utility.

#### **Advocate for data services that support cross domain solutions**

Traditional cross domain processes have been challenging and time-consuming, with limited capabilities. Seek, develop, and advocate for secure, scalable, low-latency cross domain services for near-real-time transfer of bulk data and service requests across all fabrics.

#### **Ensure IC data is cataloged**

Ensure all IC datasets are discoverable unless exempted from discovery by ODNI in accordance with IC Policy Guidance 501.1, *Exemption of Information from Discovery*. Designate mechanisms to centrally catalog all IC data in an authoritative, machine-interpretable repository. Ensure the catalog enables dataset-level discovery, de-confliction of data acquisition efforts and duplication, and tags reflecting legal, security, data sharing, and use policies. As data is further disseminated and as access rules change, data stewards will update the catalog to reflect updated policies associated with each data set.

#### **Foster sharing and reuse of validated algorithms, analytics, and related tradecraft**

Champion the cataloging, sharing, and reuse of proven analytics, algorithms, and tradecraft across the IC IE. Expose and share procedures and capabilities that act on IC data whenever possible. Leverage emerging best practices in the IC, government, industry, and academia to support innovation in advanced analytics.

## STRATEGIC GOAL 4

### Champion a culture that encourages, and rewards data-centric behaviors that effectively balance sharing and safeguarding

The IC must evolve a culture that serves the best interests of the Community and maximizes information sharing, while ensuring appropriate protections and safeguards are in place. Rooted in the principle of *Data as an IC Asset*, cultural and structural barriers that inhibit data sharing must be overcome. Embrace data stewardship as a shared responsibility across the entire data life cycle, and apply consistent data management to lower barriers to data access. Educate the IC workforce to meet these mission needs in a data-centric environment. Accelerate the development of innovative methods and technologies with strategic partnerships among industry, academia, and government that will foster experimentation and innovation.

#### OBJECTIVES:

##### Place data at the center of conversations about mission success

Recognize that making data the foundation of all activities is a major Community transformation. Accept that meeting the challenges of cultural and process change depends on higher levels of cooperation and trust among IC elements. Develop and execute a strategic communications campaign based on stakeholder needs. Convey the need for sharing data across the IC in support of intelligence integration, and acknowledge the need to break down cultural and structural barriers that impede data-centricity. Build awareness of the entire data life cycle. Promote processes that consider their life cycle impact to data prior to its collection or acquisition to reduce duplication and realize economies of scale. Bring IC personnel at all levels to view data-centric concepts as shared responsibilities, and communicate this new strategic viewpoint as essential for fully realizing the potential of *Data as an IC Asset*.

##### Establish a common operating model that incentivizes and rewards sharing and adoption of rules for discovery, access, and subsequent use of data

Identify and reduce unnecessary cultural and structural barriers that prevent data sharing and/or data integration that no longer serve the best interests of the Community. Define a common operating model that supports the IC's needs for discovery, access, and use. Promote organizational behaviors that support data-centricity for collected, processed, and acquired data. Encourage IC elements to incentivize and reward leadership and workforce behaviors that observe IC data-centric management principles, practices, and standards.

## **Establish data-related roles and responsibilities to support the complete data life cycle**

Create and leverage standards for roles and responsibilities that guide the execution of data life cycle activities across the IC, in accordance with relevant guidance. Align data-related roles and responsibilities to a common data lexicon that encompasses data science, data management, information security, civil liberties and privacy, and information management by the workforce. Establish and sustain relationships with data providers and consumers to understand the challenges they face, and define the skills and competencies required. Drive the integration of roles and responsibilities into the workflows of consumers, producers, analysts, information technologists, and policy professionals.

## **Shape data-related education, awareness, training, and development**

Advance the data-related knowledge and skills of the IC workforce by facilitating the development and sustainment of education, training, and awareness programs for collectors, data stewards, data engineers, data scientists, library scientists, archivists, and others who play a role in the data life cycle. Identify specific competencies, occupations, and career paths, and guide career development to support the data workforce. Leverage academic and industry partnerships, and IC centers of excellence, to develop data-related workforce training and awareness programs. Use the results of stakeholder needs analysis to improve strategies to promote awareness and understanding of effective stewardship behaviors across the data life cycle.

## **Harness expertise of government, industry, academia, and international partners**

Enhance partnerships with government, industry, academia, and the international community so that the variety and availability of data meets the national security challenges now and in the future. Develop new relationships and feedback loops with data providers and consumers to improve the IC's ability to accurately understand and measure mission user needs. When appropriate, collaborate with partners across the whole of government to align data-related initiatives that harmonize policies, standards, guidelines, and technical specifications while minimizing barriers and maximizing data sharing to intelligence missions.





## THE WAY AHEAD FOR STRATEGIC IMPLEMENTATION

Implementing the IC IE Data Strategy is an evolving process that requires collaboration across a range of policy, governance, management, mission engagement, and technical needs. This evolution consists of consensus building focused on championing IC element successes into Community successes. IC elements help drive successes in areas of common concern guided by the leadership of the DNI, IC CDO, and IC ISSE with support from ODNI components. IC elements will continue to implement agency-level data life cycle-related activities in accordance with all applicable legal and policy requirements, including those pertaining to the protection of privacy and civil liberties.

Even though IC data is dispersed across the IC IE, and in IC element-unique environments, it must nevertheless be discoverable, accessible, retrievable, and protected for a full range of uses. As the demand for integrated intelligence continues to expand, the Community's achievement of a data-driven culture will better enable the insights essential to overcoming our most pressing challenges.

Across its workforce, the IC must evolve and promote training and awareness to produce data-literate employees who can identify trends, visualize results, and communicate about how commingled data supports a particular analysis or intelligence insight. Success demands that the IC build and incentivize agility and flexibility into how the workforce responds to changes in technology and mission needs, which will drive changes to how the IC adapts, collaborates, creates, and adopts a data-centric culture.

Strategic partnerships between data providers and consumers are a cornerstone of this strategy, enabling a shared understanding of the unique mission challenges users face in every analytic and decision-making environment. Fully realizing a data-driven culture will require the strong foundation of a continuing commitment from senior leadership across the IC to drive the transformation necessary to achieve shared responsibility for the data life cycle.

The execution of this strategy requires consistent governance, collaborative assessment, and continuous process improvement to demonstrate progress against the goals and objectives. The IC CDO and the IC ISSE collaborate with IC elements to realize an IC-wide strategic direction for enterprise data and information sharing. The IC CDO Council and the Information Sharing Steering Committee are the two primary governance bodies who will oversee and prioritize implementation of the principles in the IC IE Data Strategy.









**IC IE DATA STRATEGY  
2017-2021**