Office of the Director of National Intelligence

(U) Intelligence Community Enterprise Architecture (IC EA):

IC Data Reference Architecture (DRA) Strategic Elements Document

LEADING INTELLIGENCE INTEGRATION

24 March 2021

This Page Intentionally Left Blank

Ms. Nancy E. Morgan

Intelligence Community Chief Data Officer

Nancy Ellis Morgan

Date 03/25/2021

Mr. Michael E. Waschull

Acting, Intelligence Community

Chief Information Officer

Mike Waschull

Date 3/25/21

(U) Change Log

Date	Author/Email/Org	Change Summary	Section	Issuance Date
18-Oct-2019	[redacted]	Incorporated comments resulting from 3-day Strategic Elements offsite sessions	All, see comments adjudication file	Preliminary Draft 18-Oct-2019
11-Dec-2019		Incorporated comments resulting from review by NSA and IC CDO teams	All, see comments adjudication file	Draft 11-Dec-2019
22-Jan-2020		Incorporated comments from Steven W. Harper (934-3340) ODNI/EC/IC CIO/COS	All, see comments adjudication file	Draft 22-Jan-2020
04-Feb-2020		Incorporated comments from January 2020 CDOs offsite	Positions, Data Patterns	Draft 04-Feb-2020
24-July-2020		Incorporated comments resulting from Dec-2019 to Feb 2020 Formal Coordinated Community review tasker	All, see comments adjudication file	Draft 24-July-2020
24-Aug-2020		Incorporated comments from IC CDO, IC CDO deputy, AIG contractor DRA Lead, AIG Contractor Technical Director, and AIG routing approval personnel	All, see comments adjudication file	Draft 24-Aug-2020
16-Sep-2020		Incorporated comments from IC TIC NG	All, see comments adjudication file	Final 16-Sep-2020
28-Sep-2020		Incorporated comments from NSA Chief Architect, Chief Information Security Officer, and Chief Data Officer	Executive Summary, 1 /Introduction , 7 /Acronyms , see comments adjudication file	Final 28-Sep-2020
20-Nov-2020		Incorporated comment #384 from Brian Ince (ODNI/CLPT)	Executive Summary, 1 /Introduction , 7 /Acronyms , see comments adjudication file	Final 20-Nov-2020
09-Feb-2021		Incorporated comments from DNI/GC/MGMT, Laura Casulli	Various sections, see comments adjudication file	DRA SED 11/20/2020_CDOC vote Version
17-Feb-2021		Incorporated comments from DNI/GC/MGMT, Laura Casulli and DNI/CIO/AIG Tammy Osborn.	Various sections, see comments adjudication file	DRA SED 11/20/2020_CDOC vote Version
04-Mar-2021		Incorporated comments for clarity and correctness from Ms. Nancy E. Morgan, IC CDO and the IC CDO team	Various sections, see comments adjudication file	2020_02_24_DRA Strategic Elements Document Final_1128hrs

(b)(3)
(b)(6)

(U) Executive Summary

(U//~~FOUO~~) The Intelligence Community (IC) and Department of Defense (DoD) operate in a geographically dispersed, information-rich environment in which United States (U.S.) and non-U.S. personnel work. Missions are accomplished across Top Secret/Sensitive Compartmented Information, Secret, and Unclassified security fabrics, including coalition and allied fabrics. Enabling effective operations in this environment requires an IC Data Reference Architecture (DRA) that facilitates data sharing, interoperability, standard practices, and analytic innovation. A well-designed DRA also enhances safeguarding and information integrity in the IC Information Environment (IE).

(U//~~FOUO~~) The DRA fulfills a key objective of the IC IE Data Strategy 2017-2021 first strategic goal, which is to "Establish a common reference data architecture" which "provides detailed architectural information in compatible formats to enable solutions to be repeatedly designed and deployed in a consistent, high-quality, and supportable fashion." This includes transitioning to a data-centric enterprise; decoupling data from specific applications and environments (e.g., data are immutable to changes in applications and associated execution states/conditions); reusing/redesigning solutions for different intended uses; and fostering increased and more secure data sharing. Apart from satisfying the IC IE Data Strategy goals and objectives, the DRA addresses data concepts relating to the evolving digital engineering/model-based systems engineering domain.

(U) The DRA details the architecture and minimum interoperability standards required to enable increased: data sharing/reuse, data safeguarding, cross-IC intelligence integration, data/information assurance, and support for all phases of the data lifecycle.

(U) IC data subject matter experts (SMEs) and stakeholders collaborate with the IC Chief Information Officer (CIO) and IC Chief Data Officer (CDO) personnel as a virtual team. The DRA government lead, as a member of the Office of the Director of National Intelligence (ODNI) Intelligence Community Chief Information Officer (IC CIO) Architecture and Integration Group (AIG), is the overall point of contact in the organization responsible for change management, maintenance, and availability of this document. The DRA can be routinely used by IC data stewards and other IC data professionals and provides data solutions implementation guidance to enable operational advantage through intelligence superiority.

(U) Table of Contents

(U) List of Figures

(U) List of Tables

1 (U) Introduction

(U) The IC has established a Reference Architecture (RA) Framework (RAF) process to guide the consensus development of specific RAs. The RAF is a process, not a document. The RAF process is a living process.

(U//~~FOUO~~) The DRA adheres to the RAF process, however as of the signed date of the Strategic Elements Document, the members of the IC Chief Data Officer (CDO) Council (CDOC) expressed their preference for the DRA to not have a section titled "Strategic Patterns" or "Scope and Patterns," but to have a section titled "Patterns."

(U) The RAF process is not intended to infer formality and authority of the RAF process beyond developing RAs. The RAF is a process for enterprise capability, planning, and execution. The RAF process is managed and directed by the ODNI/IC CIO/AIG organization leadership.

(U) The RAF process includes developing several RA artifacts to guide operational outcomes, including documenting the touchpoints and interdependencies for RAs. The first artifact in an RA is a main document that presents five key strategic elements:

- Strategic purpose and scope;
- Principles;
- Positions;
- Patterns; and
- Vocabulary.

(U//~~FOUO~~) The IC IE Data Strategy 2017-2021calls for the DRA to "Establish standards that are scalable and agile, built on the concept of data-centricity to facilitate extraction of data . . . to a range of uses as internal and external needs change."

(U//~~FOUO~~) The DRA details the minimum best practices and architectural guidance to promote the principle of managing "data as an IC asset" as referenced in the IC IE Data Strategy 2017-2021. Further, the DRA supports the IC IE Data Strategy's vision statement to get "the right data, to the right people, at the right time, in the right form."

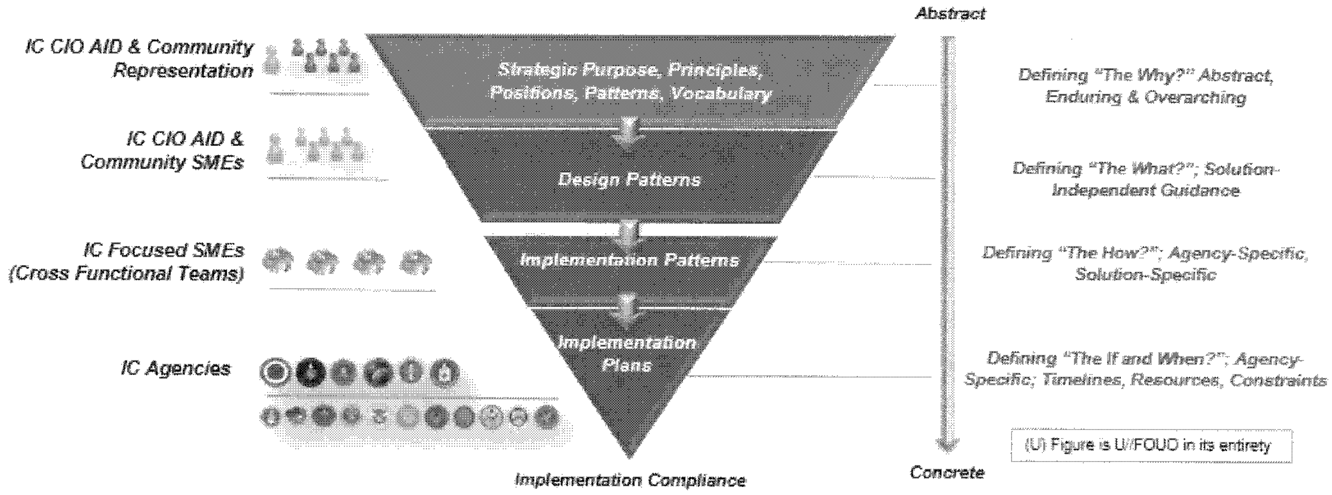
(U//~~FOUO~~) The IC is transitioning to a federated, data-centric information environment. The community handles numerous types of data from multiple sources on various security domains. Data capabilities are hosted on one or more cloud(s) both on and off-premise, and in non-cloud environments on premise at IC element locations, in multi-fabric environments. Data is shared to the maximum extent possible within the legal, policy, oversight, and compliance framework while being fully protected.

(U//~~FOUO~~) Addressing data-protection issues during the RA stage, rather than adding an unwieldy layer of legal compliance to a near-final system, is increasingly recognized as the right approach to security and privacy engineering. Data-driven services and products must:

- Safeguard all data sets including those that may contain personally identifiable information (PII);
- Fulfill current compliance obligations, as well as future-proofing products and services to meet these obligations in a changing technological and policy environment; and
- Facilitate communication between Chief Data Officers, Civil Liberties, Privacy and Transparency (CLPT) Officers, data stewards, mission partners, business partners, security assessors, and other stakeholders.

1.1 (U) DRA Linkage to the RAF Process

(U) The following RAF process figure represents a consistent, repeatable, and verifiable process for developing and applying RAs in the IC.


Abstract
IC CIO AID & Community Representation
Strategic Purpose, Principles, Positions, Patterns, Vocabulary
Defining "The Why?" Abstract, Enduring & Overarching
IC CIO AID & Community SMEs
Design Patterns
Defining "The What?"; Solution-Independent Guidance
IC Focused SMEs (Cross Functional Teams)
Implementation Patterns
Defining "The How?"; Agency-Specific, Solution-Specific
IC Agencies
Implementation Plans
Defining "The If and When?"; Agency-Specific; Timelines, Resources, Constraints
Implementation Compliance
Concrete

(U) Figure is U//FOUD in its entirety

Figure 1 (U) Applying the RAF process

(U//~~FOUO~~) Figure 1 illustrates a repeatable approach for applying RAs in the IC for achieving operational, interoperability, and security objectives. Generically, the model is represented as an inverted triangle with four discrete layers. These include (starting from top to bottom):

- First tier (illustrated in purple): The strategic elements represent abstract, overarching and enduring content of the RA including: strategic purpose, principles, positions, patterns, and vocabulary. These are key content items of any IC RA.
- Second tier (illustrated in blue): A design pattern is a general, reusable integration solution to a commonly occurring problem within a given context of a service area (e.g., unified communications). In essence, design patterns illustrate and describe the "what" of

integration. Design patterns are drafted as part of a native RA but are delivered as independent addendums to the overarching RA document to support focused distribution and use. The combination of the top two tiers represent the entire RA.

- Third tier (illustrated in aqua): Implementation patterns describe specific solutions that instantiate a design pattern. Community SMEs for specific service areas develop implementation patterns that account for the IT and policy constraints of each agency. In this way, implementation patterns extend design patterns in that they illustrate and describe the "how" of integration.
- Fourth tier (illustrated in green): IC agencies develop specific implementation plans that describe the "if and when" details for complying with specific implementation patterns. These plans provide each agency with a realistic approach for achieving interoperability.

(U) The models all drive towards "implementation compliance." By using this process, all RA conforming implementations should be interoperable and provide for secure DRA services and drive out enterprise-driven operational capabilities across the IC.

1.2 (U) DRA Dependencies with Other RAs

(U) The DRA is dependent upon external components outlined within existing and future RAs. As services evolve within the IC EA, the DRA will more clearly define these dependencies across traditional boundaries. Figure 2 illustrates that the application of the DRA to develop secure and interoperable communication and collaboration solutions is dependent on both the Identity, Credential, and Access Management Reference Architecture (ICAM RA) and the Collaboration Reference Architecture (CRA). Examples of potential dependencies between DRA and ICAM RA include: data storage security; data service security; data policies; and protecting compartmented data. Examples of potential dependencies between DRA and CRA include: data services integration with presentation tools and email services. The DRA is to be iterative and evolve as the needs of its stakeholders change.

(U) Figure is U//~~FOUO~~ in its entirety

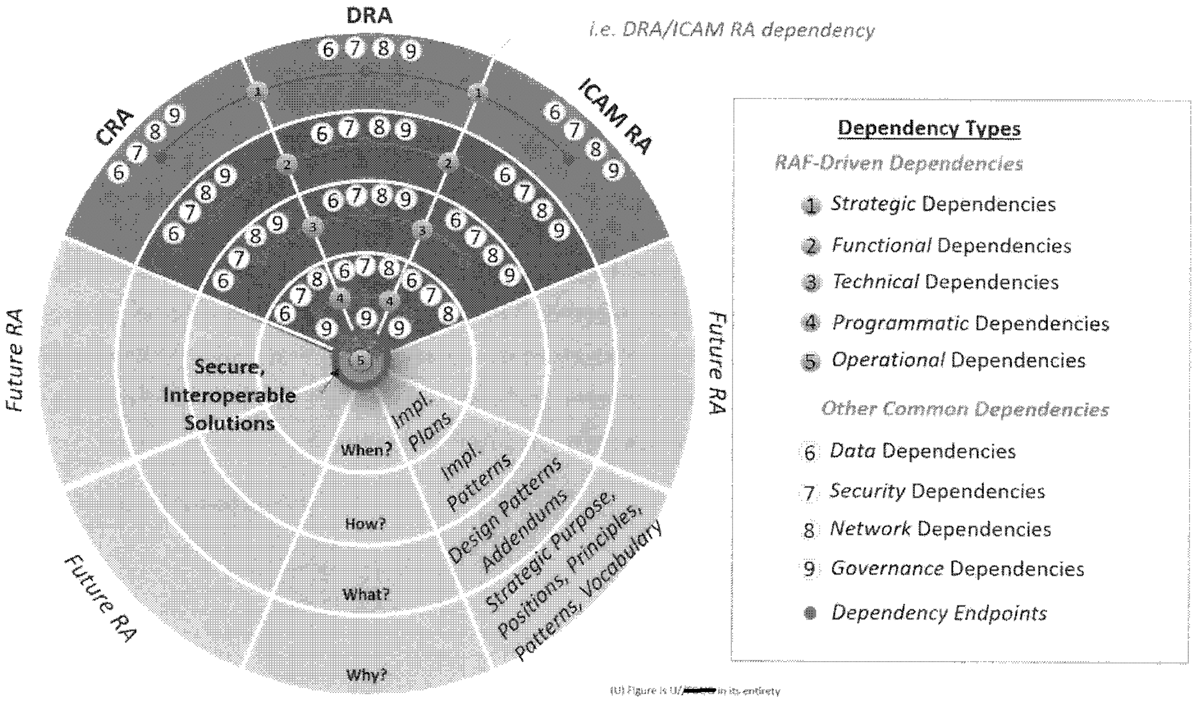

DRA
i.e. DRA/ICAM RA dependency
CRA
ICAM RA
Future RA
Future RA
Future RA
Secure, Interoperable Solutions
When?
How?
What?
Why?
Impl. Plans
Impl. Patterns
Design Patterns Addendums
Strategic Purpose, Positions, Principles, Patterns, Vocabulary
Dependency Types
RAF-Driven Dependencies
1 Strategic Dependencies
2 Functional Dependencies
3 Technical Dependencies
4 Programmatic Dependencies
5 Operational Dependencies
Other Common Dependencies
6 Data Dependencies
7 Security Dependencies
8 Network Dependencies
9 Governance Dependencies
● Dependency Endpoints
(U) Figure is U//~~FOUO~~ in its entirety

Figure 2 (U) Dependencies Relationships

1.2.1 (U) Dependencies Terminology

(U) The RAF process-driven dependencies mirror the IC RAF process pyramid outlined in Figure 2 . As an RA transitions from the strategic purpose ("Why?") phase to the implementation plans ("When?") phase, dependencies, from one RA to another RA, are identified. The RAF process-driven dependencies include:

- Architecture strategic integration dependencies ("Why?"): Shared/common principles and vocabulary between RAs;
- Architecture functional integration dependencies ("What?"): Process-level dependencies between RAs (This level of integration is described in RA design patterns);
- Development technical integration dependencies ("How?"): Technical behavior-level dependencies where the "success" of one technical service is dependent on the outputs/results provided by another technical service (this level of integration is described in RA implementation patterns);
- Development programmatic integration dependencies ("When?"): Resource, schedule, budget dependencies between agencies (this level of integration is addressed in IC Element implementation plans and joint integration plans); and

- Development operational integration dependencies: Solution-level dependencies in the run-time operational environment (this level of integration is managed as enterprise configuration items).

1.3 (U) DRA Governance Business Process Modeling Notation (BPMN)

(U//~~FOUO~~) The ODNI IC CIO AIG developed a standardized governance process for officially approving and releasing RAs using the RAF process. The initial development of each RA is coordinated with IC stakeholders using a combination of off-sites and working group meetings to drive the process. When the RA is finished, review and consensus with the IC stakeholders is achieved, the RA progresses through the workflow outlined in Figure 3.

(U) Figure is U//~~FOUO~~ in its entirety

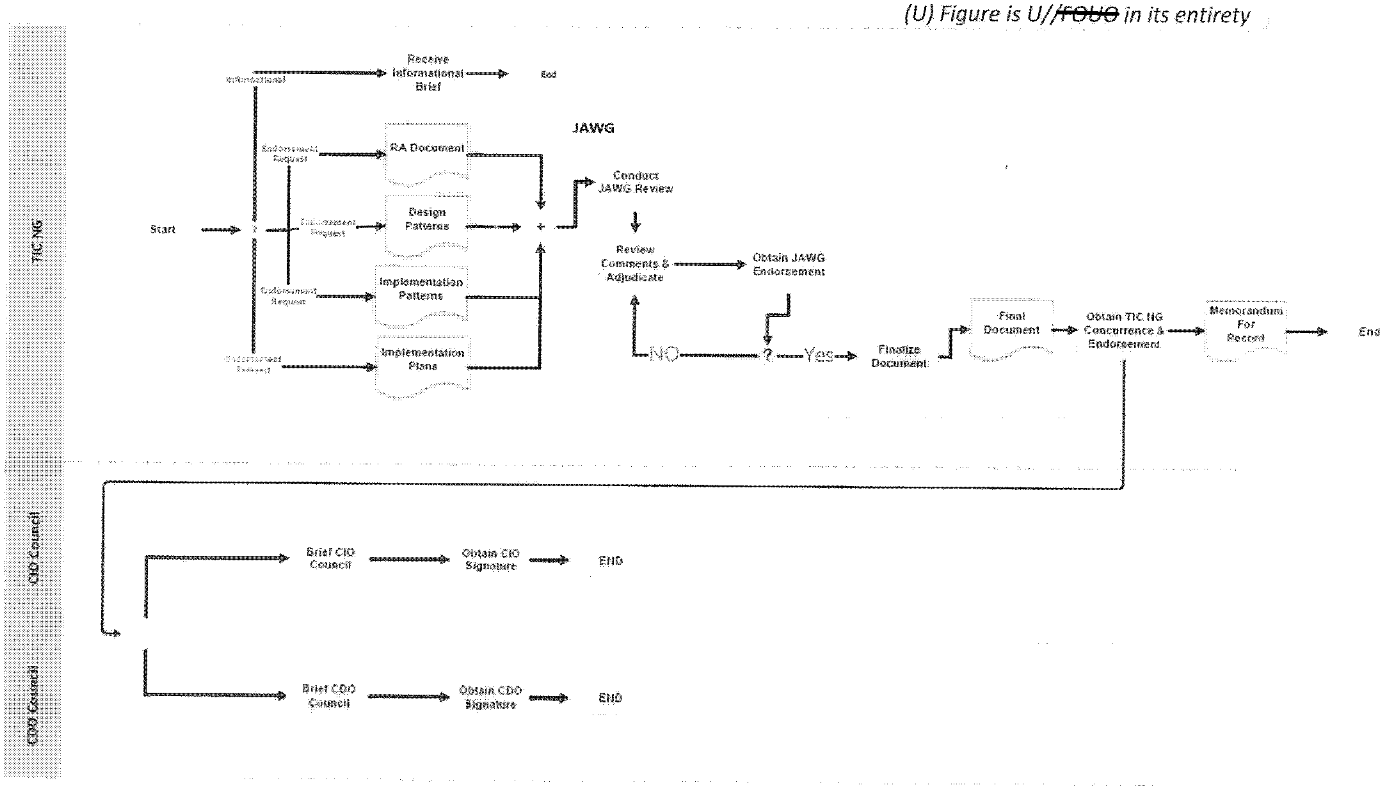


Figure 3 (U) DRA Governance BPMN

(U//~~FOUO~~) The DRA governance cycle typically includes briefings to the IC Joint Architecture Working Group (IC JAWG), IC Technical Integration Committee Next Generation (IC TIC NG), the IC CIOC, and IC CDOC. The Director of ODNI/IC CIO/AIG has the authority to decide whether an IC JAWG review is required. Once approved, the DRA is signed by the IC CIO and the IC CDO. As alterations to the document are necessary, the changes are brought through the IC stakeholder review processes and the governance cycle to be approved as a different incremental RA version. IC stakeholder coordination will occur as needed throughout the governance process. Impact to current implementations are evaluated at that time, and the IC CIO and the IC CDO will then issue implementation direction.

2 (U) Strategic Purpose and Scope

> *(U) "Provide timely, insightful, objective, and relevant intelligence and support to inform national security decisions and to protect our Nation and its interests."*
>
> - IC Mission, 2019 National Intelligence Strategy

(U//~~FOUO~~) The IC IE Data Strategy 2017-2021 mission statement describes success as dependent upon the ability to "make IC data more discoverable, accessible, and usable at the speed of mission." A key objective of the data strategy is to establish a common DRA. The DRA's goal is to enable capabilities to be designed and deployed repeatedly in a consistent, high-quality, and supportable fashion.

(U) Consistent with their mission, IC elements regularly acquire data from outside the IC by a variety of arrangements, such as purchase from commercial providers, agreements with federal departments and other agencies, or by foreign partner exchange. Within the context of the IC data acquisition strategy going forward, IC elements continue to make best efforts to negotiate and make information maximally available for all applicable IC missions consistent with applicable laws and policies that flow through our complex ecosystem. In addition to the IC IE Data Strategy goals, requiring a DRA, additional rationales include the need for a RA that contributes to enabling expanded IC sharing of acquired data as well as the growing demand for additional data sets from federal, state, local, tribal, foreign, and private sector partners.

(U//~~FOUO~~) The DRA provides the guidance to facilitate information sharing, enhanced safeguarding, and intelligence integration to meet intelligence needs. Specifically, the DRA:

- Encourages a cultural shift driving towards the holistic use of data to enable higher-quality intelligence;
- Provides guidance to balance the needs of IC elements and IC partners with the needs of the IC as a whole;
- Promotes data-centricity within the IC IE and with IC partners to support information sharing, integration, and secure data exchange;
- Facilitates data usability/reusability, reliability, fidelity, and manageability; and

- Builds privacy data requirements into the RAs to promote the successful and consistent incorporation of privacy data practices into an organization's mission and business activities, processes, and services.

2.1 (U) DRA Scope

(U) In the RAF process, "scope" refers to the enduring sphere of influence the RA seeks to affect. Scope is broad and strategic and is not specific to any RA version. The strategic purpose (purple, top level) phase documents the scope of the RAF process as illustrated in Figure 4.

(U) Figure is Unclassified in its entirety

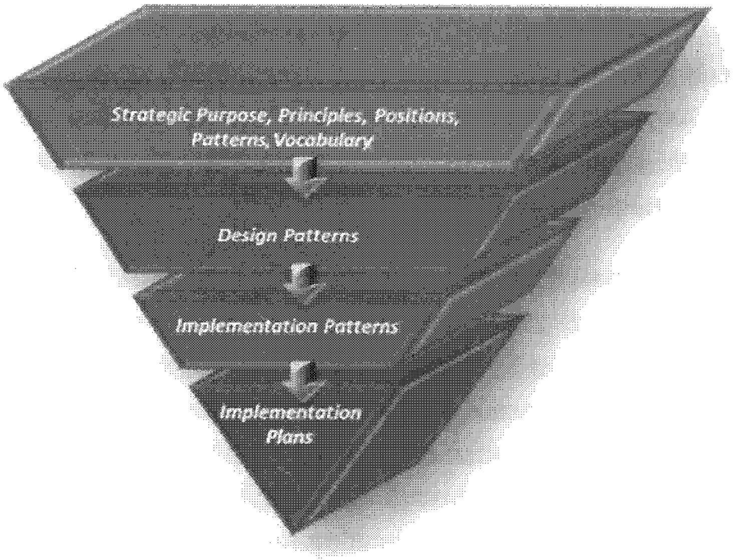

Strategic Purpose, Principles, Positions, Patterns, Vocabulary
Design Patterns
Implementation Patterns
Implementation Plans

Figure 4 (U) IC RAF process

(U) The DRA's scope is characterized by specific parameters, including the overall enterprise, supported partnerships, consumers, providers, fabrics, lines of business (LoB), and operational modes. DRA's scope is described in terms of desired outcomes. For a description of parameters of the DRA scope and key DRA enabled outcomes, refer to the glossary.

2.2 (U) IC Data Management Lifecycle Wheel

(U) The IC Data Management Lexicon (DML) defines the data lifecycle as "a conceptualization of a birth-to-death value chain for data, which often includes phases such as plan and task, acquire and assess, process and transform, discover and access, analyze and exploit, and preserve or dispose."

(U) The IC Data Management Lifecycle Wheel is included here so that the reader can view and better understand the phases of data. Although the data lifecycle wheel phases are defined in the vocabulary section of this DRA document, those definitions are also duplicated here so the reader can better understand the phases of data within the context of this section of the DRA document.

(U) Figure is Unclassified in its entirety

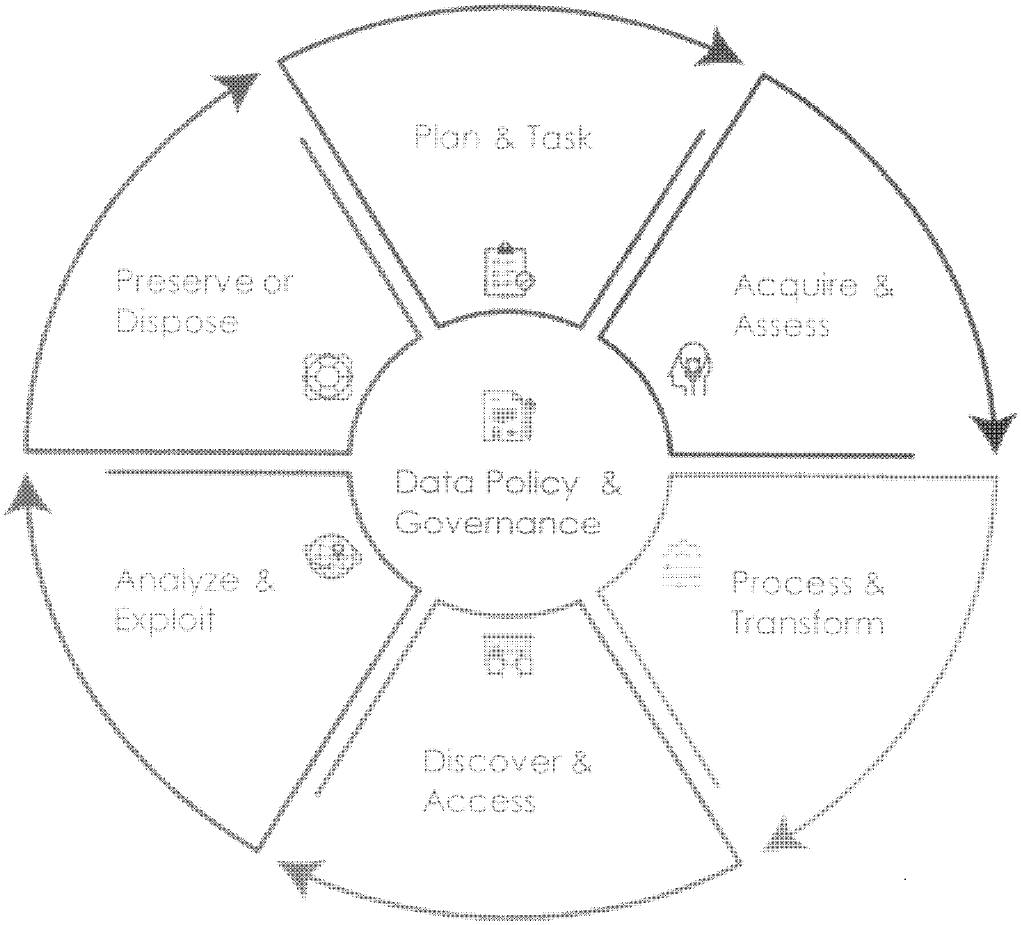


Figure 5 (U) IC Data Management Lifecycle Wheel

(U) The following data lifecycle wheel definitions are sourced from the IC DML IC Standard (ICS) 501-01 and were approved and baselined by the IC CDOC:

(U) **Plan & Task** - Activities prior to obtaining data that include how data needs are determined; collection objectives are prioritized; costs, storage and compute requirements are assessed; collection methodologies or approaches are selected; and decisions are documented with respect to relevant data authorities, permissions, and use and sharing rules.

(U) **Acquire & Assess** - Activities related to procurement, collection, and generation of data, including determining mission-relevant features or business purposes. This phase includes:

- Ensuring source vetting;
- Validating and verifying data;
- Evaluating preliminary data quality;
- Identifying filtering and PII minimization and data volume-reduction opportunities; and
- Documenting data impact assessments on all data sensitivities, handling, use, protection, and disposition requirements.

(U) **Process & Transform** - Activities and documentation related to making data fit for purpose (e.g., data conditioning) and fostering data interoperability across systems. This phase includes aspects of data curation to describe data and enhance discoverability.

(U) **Discover & Access** - Activities that ensure data can be found by and made available to any authorized consumer, and protected through policies for access control and need-to-know. This starts dissemination (per ICD 501) for data that is made accessible outside of an IC element.

(U) **Analyze & Exploit** - Activities related to the use of data for mission purposes. These activities ensure the usability of data by specific tools, performance of data gap identification, continued data safeguarding through data handling and usage limitations, and determination of data value. Data value is derived through targeted queries, analytic models, and automated analytic capabilities (e.g., data correlation, data fusion) while preserving provenance, pedigree, and lineage. This phase also serves as the foundation for intelligence dissemination determinations and tradecraft.

(U) **Preserve or Dispose** - Activities related to final data disposition. This includes preservation, purge, or deletion performed in accordance with National Archives-approved records control schedules, legal hold requirements and references and lawful guidance such as the Attorney General Approved Guidelines Pursuant to Executive Order (E.O.) 12333 and Presidential Policy Directive 28.

(U) **Data Governance** - Discipline comprised of responsibilities, roles, functions, and practices, supported by authorities, policies, and decisional processes (planning, setting policies, monitoring, conformance, and enforcement), which together administer data and information assets across an IC element to ensure that data is managed as a critical asset consistent with the organization's mission and business performance objectives.

3 (U) Principles

(U) The principles define the precepts that guide direction of the DRA. The terms with identifiers (ID) D-01 through D-08, align to the Data Management Association (DAMA) Data Management Body of Knowledge (DMBoK) and the DAMA Dictionary. Terms only deviate from these sources when there is a rationale (per CDOC) or per definitions of data terms (see section 6.4). Data architecture frameworks, taxonomies, and ontologies are also important aspects to guide architecture direction. For completeness, the DoD Architecture Framework, the Unified Architecture Framework, and the Federal Enterprise Architecture are also referenced in this section. The following table contains the principles that span all RAs and those that are pertinent to data in particular. (Key: ***G****=Guiding,* ***C****=Corporate,* ***A****=Architecture,* ***D****=Data).*

(U) Table is Unclassified in its entirety

ID	Principle
G-01	The RAF process is the primary guide for developing an IC-wide enduring commitment to these principles.
G-02	IC IT operates as a federation enabler.
G-03	RAF process maximizes use of existing efforts.
G-04	Outcomes and environmental factors guide the use of federation or integration of data.
C-01	IC elements build to share.
C-02	IC elements build to support change.
A-01	Enhanced capabilities do not break mission.
A-02	The DRA coordinates with other RAs.
A-03	The DRA focuses on "cross-community" data.
A-04	The DRA focuses on secure interconnections using existing services.
D-01	Applicable authorities govern the stewardship of data.
D-02	The IC IE is a data-centric[1] enterprise.
D-03	IC information exchange, interface standards, and specifications are foundational for interoperability.
D-04	The IC data lifecycle,[2] applicable laws, policies, and compliance rules, guide and constrain IC data-management processes and activities.
D-05	Each IC element protects, shares, and manages IC data wherever it is located across the enterprise.
D-06	All authorized consumers can discover IC data.
D-07	The development and application of IC data-tagging standards and data protection policies (for both lifecycle management functions as well as for context) are essential for interoperability.
D-08	Manage all data as an IC asset.

Table 1 (U) IC DRA Principles

[1] (U) Defined by the IC DML Working Group (IC DML WG).

[2] (U) Defined by the IC DML WG, in compliance with applicable laws, regulations, and policies.

3.1 (U) Guiding Principles

- **(U) G-01: The RAF process is the primary guide for developing an IC-wide enduring commitment to these principles.**
  - **Statement:** The DRA is a community-developed, community-owned RA. Achieving the DRA objectives is only possible if all agencies are committed to its development, maintenance, and conformance. The drivers for DRA success are:
    - Strong executive sponsorship;
    - Committed service providers with functional roadmaps;
    - Phased approach implementation; and
    - Engaging users at all levels of the organization in the implementation process.

- **(U) G-02: IC IT operates as a federation enabler.**
  - **Statement:** The governance model for the DRA is a lightweight, central facilitation and coordination of the DRA implementation components. The IC will leverage enterprise services to implement and operate solutions.

- **(U) G-03: RAF process maximizes use of existing efforts.**
  - **Statement:** There are a great deal of established solutions, working groups, SME resources, etc. to provide services today. The DRA approach is to leverage, and re-purpose where appropriate, this infrastructure as much as possible.

- **(U) G-04: Outcomes and environmental factors guide the use of federation or integration of data.**
  - **Statement:** Mission requirements and environmental factors dictate whether federated or integrated data approaches need to be applied. The DRA supports both and fosters ensuring the pedigree of federated and integrated data during maintenance. Mission needs drive data-duplication decisions. The creation of data occurs in many places and movement of data happens between many places. Coordinating work processes and maintaining alignment of end results requires planning from an architectural and from a workflow process perspective.
  - *Source: Derived from DMBOK, Data Management Overall [pp. 21-23].*

3.2 (U) Corporate Principles

- **(U) C-01: IC elements build to share.**
  - **Statement:** Systems and applications in the IC need to be accessible via a universally available IP network, playing the role of the internet. Access to the data may be limited by policy, but not by limiting access to the application. Users should be able to use any properly approved application to process any data to which they have access, and be unable to access unauthorized data. To ensure applications and components of applications are shareable, the IC elements will use a common application development and composition framework based on rapidly evolving web standards. Device and location independence allows reuse of applications and data across environments.

- **(U) C-02: IC elements build to support change.**
  - **Statement:** IT services and IT developers who consume IT services, must be prepared to maintain a level of abstraction and preparation for constant change in internal interfaces without affecting end users. Decomposition into services has to ensure that the decoupling of interfaces are at well-developed, natural points of demarcation in the IT industry. Layers of abstraction and clean interfaces enable evolution and scalability of services.

3.3 (U) Architecture Principles

- **(U) A-01: Enhanced capabilities do not break mission.**
  - **Statement:** Do not encumber the mission with additional steps or procedures. The intent of this effort is to provide security, technical, and operational enhancements for secure cross-Community, user-to-user collaboration and data-sharing capabilities, without causing any degradation, or negative impacts, to any IC mission or operation.

- **(U) A-02: The DRA coordinates with other RAs.**
  - **Statement:** There are several RA efforts (e.g., ICAM RA and CRA) underway where close coordination is required so that references from one RA to content in another RA are used, rather than covering the same material in two separate RAs.

- **(U) A-03: The DRA focuses on "cross-community" data.**
  - **Statement:** The DRA deals with the IC; thus, the interoperation across the IC is the boundary of the DRA.

- **(U) A-04: The DRA focuses on secure interconnections using existing services.**

- **Statement:** The focus of this effort is the interconnection of user collaboration and data-sharing services. Additionally, all IC collaboration endpoints must implement security policies, standards, and records management requirements.

3.4 (U) Data Principles

- **(U) D-01: Applicable authorities govern the stewardship of data.**
  - **Statement:** Maintenance of organizational control (stewardship) over data is a prerequisite for information sharing between organizations. Laws, authorities, policies, standards, and specifications establish and constrain the stewardship of data.
  - *Source: Derived from ICAM RA Final, 26 July 2019, Principle I-07, pp. 18-19.*

- **(U) D-02: The IC IE is a data-centric enterprise.**
  - **Statement:** Data is de-coupled from specific systems, services, applications, and/or environments. Rules (e.g., data protection, data handling, authorities, retention, etc.) are associated with data to support maximum utility and portability.
  - *Source: Derived from IC data stakeholders' strategic elements offsite direction.*

- **(U) D-03: IC information exchange, interface standards, and specifications are foundational for interoperability.**
  - **Statement:** The IC IE requires enterprise standards that are extensible and define the characteristics of services as well as the flow, control, and secure exchange of information. This principle applies to the interfaces and exchanges (including data syntax and format) of controls, requests, and responses.
  - *Source: Derived from ICAM RA Final, 26 July 2019, Principle I-05.*

- **(U) D-04: The IC data lifecycle, and applicable laws, policies, and compliance rules, guide and constrain IC data management processes and activities.**
  - **Statement:** The IC data lifecycle results in the establishment and execution of policies and interconnected processes for managing data throughout the data lifecycle to support data management functions, such as data governance.
  - *Sources: Adapted from DMBOK, 2nd Edition, p.23, IC CDO Council-approved Data Lifecycle, and derived from IC DML.*

- **(U) D-05: Each IC element protects, shares, and manages IC data wherever it is located across the enterprise.**
  - **Statement:** The DRA enables capabilities and processes that control and protect data in accordance with laws, authorities, and policies, including across domains and fabrics. The implementation of a resilient, documented, and scalable architecture based on shared best practices and common standards is critical to the IC.
  - *Source: Derived from IC IE Data Strategy 2017-2021, restatement of Strategic Goal 2.*

- **(U) D-06: All authorized consumers can discover IC data.**
  - **Statement:** Understanding that some IC data is "exempt" from discovery, all "authorized" consumers can obtain knowledge of the existence, but not necessarily the content, of information (data) collected or of analysis produced by any IC Element.
  - *Sources: Inspired from IC IE Data Strategy, Strategic Goal 3, and derived from ICD 501.*

- **(U) D-07: The development and application of IC data-tagging standards and data protection policies (for both lifecycle management functions as well as for context) are essential for interoperability**.
  - **Statement:** The IC must develop and apply common data-tagging[3] standards to enable key data lifecycle functions (e.g., discovery, access, access control, protection, and use of business and mission data) as well as to facilitate context (e.g., entity, analytic, semantic, and syntax standards). Implementing an interoperable, comprehensive data-tagging methodology that complies with IC standards for core-data lifecycle functions is essential for IC IE operations.
  - *Source: Derived from IC IE Data Strategy 2017-2021, Strategic Goal 1, Objective 4.*

[3] (U) Defined by the IC DML Working Group

- **(U) D-08: Manage all data as an IC asset.**
  - **Statement**: 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. Each IC element will be able to validate that they fulfill all obligations related to data handling and retention. Accelerate the development of innovative methods and technologies with strategic partnerships among industry, academia, and government to foster experimentation and innovation.
  - *Source: Derived from IC IE Data Strategy 2017-2021, Strategic Goal 4.*

4 (U) Positions

4.1 (U) Positions Introduction

(U) The DRA positions section summarizes strategies and initiatives that drive or guide the accomplishment of objectives, increase effectiveness, promote integration, and achieve efficiencies to operationalize strategic initiatives and priorities for the IC.

4.2 (U) Data Positions

(U) The following table lists primary strategies and initiatives relevant to the DRA strategic elements. Federal laws, IC guidance, and IC directives relevant to the DRA strategic elements are listed in the reference section of this document.

(U) Table is Unclassified in its entirety

ID	Title	Description
(U) Federal Data Strategy	(U) Federal Data Strategy – A Framework for Consistency, June 4, 2019	(U) This strategy provides a common set of data principles and best practices to implement data innovations that drive more value for the public. Its three components guide federal data management and use: Mission statement, principles, and practices. [Source: Executive Office of the President Office of Management and Budget, Federal Data Strategy–*A Framework for Consistency, Memorandum for the Heads of Executive Departments and Agencies,* June 4, 2019, M-19-18]
(U) IC IE Data Strategy (2017-2021)	(U) Intelligence Community (IC) Information Environment (IE) Data Strategy 2017-2021	(U) The IE Data Strategy guides the IC toward a common, more secure and integrated enterprise by using the vision and framework of the IC IE to operationalize a data-centric community. It calls upon IC elements to place mission and business data at the center of every plan to drive mission success. [Source: ODNI/IC CIO/AIG, *Collaboration Reference Architecture Final*]

ID	Title	Description
(U) IC IE FY 17-18 Baseline	(U) Intelligence Community (IC) Fiscal Year (FY) 17-18 Baseline	(U) This document introduces the overarching IC EA framework and describes how IC information technology enterprise fits into the broader IC EA as the end of FY2016.
(U) IC EA: CRA	(U) Intelligence Community (IC) Information Environment (IE) Collaboration Reference Architecture (CRA)	(U) This document provides foundational guidance (minimal IC service configuration and interconnection standards) for realizing secure interoperability across the IC's federated communication and collaboration solutions.
(U) IC EA: ICAM RA	(U) Intelligence Community (IC) Information Environment (IE) Identity, Credential, and Access Management Reference Architecture	(U) This document provides a tie between the pure strategic ICAM view expressed in the IC ICAM Security Segment Framework to a more tactical, version specific design view for a given set of outcome(s) to be addressed to either provide new capabilities or improve upon existing ICAM service(s). The document describes the community identified design patterns for this specific version of ICAM RA.
(U) National Cyber Strategy	(U) National Cyber Strategy of the United States of America, September 2018	(U) This strategy aligns risk management and information technology activities in accordance with E.O. 13833, *Enhancing the Effectiveness of Agency Chief Information Officers (CIOs)*. It empowers CIOs to more effectively leverage technology and accomplish agency missions, cut down on duplication, and make IT investment more efficient. [Source: *National Cyber Strategy of the United States of America*, The White House, September 2018, p. 16]
(U) National Strategy for Information Sharing and Safeguarding	(U) National Strategy for Information Sharing and Safeguarding, December 2012	(U) This strategy balances sharing information with those who need it to keep our country safe with protecting it from those who would do us harm. It outlines the operating environment, three principles, five goals, and the way forward. [Source: The White House, *National Strategy for Information Sharing and Safeguarding, December 2012*]
(U) NIS	(U) National Intelligence Strategy (NIS) 2019	(U) This strategy focuses IC plans and actions for four years (ending in 2023), and provides direction to guide the development of future IC capabilities. Enterprise objective five of the NIS focuses on information sharing and safeguarding. [Source: Director of National Intelligence, *2019 National Intelligence Strategy of the United States of America*, Washington, D.C. 20511, January 22, 2019]]
(U) Strategic Plan to Advance Cloud Computing	(U) Strategic Plan to Advance Cloud Computing in the Intelligence Community, June 26, 2019	(U) This document specifies seven interrelated objectives and 38 initiatives the IC must achieve to reach the cloud computing future state.
(U) Digital Government Strategy, 23 May 2012	(U) Digital Government Strategy, 23 May 2012	(U) This strategy derives from its open data component and builds on several initiatives and governance including: • E.O. 13571, *Streamlining Service Delivery and Improving Customer Service;* • E.O. 13576, *Delivering an Efficient, Effective, and Accountable Government;* • Memorandum M-13-13, *Open Data Policy—Managing Information as an Asset;* and • The goal of achieving efficiency, transparency, and innovation through reusable and open source software as described in Memorandum M-16-21, *Federal Source Code Policy.* The open data website is a collection of supporting code, tools, and case studies designed to help agencies adopt the open data Policy.

ID	Title	Description
(U) The AIM Initiative	(U) The AIM Initiative, Augmenting Intelligence Using Machines (AIM), 31 May 2016	(U) This document provides the framework for incorporating AIM technologies to accelerate mission capability development across the IC.
(U) E/S 00651	(U) Executive Series (E/S) 00651, Delegation of Intelligence Community Information Management Authorities and Responsibilities, 3 February 2012	(U) This memo establishes the responsibility of the Chief, IC Information Management, to include overseeing and providing leadership for the IC on information-management issues, including the disciplines of records management and classification management.
(U) ICS 501-01	(U) Intelligence Community Standard (ICS) 501-01	(U) On October 28, 2019, the IC Data Management Lexicon ICS 501-01 was signed by the Assistant Director of National Intelligence (ADNI) for Information and Data. The ICS outlines the process and responsibilities for identifying, approving, and managing the common terminology for data management across the IC IE.
(U) ICS 500-20	(U) Intelligence Community Standard (ICS) 500-20	(U) On December 16, 2010, the Enterprise Standards Compliance ICS 500-20 was signed by Charlene P. Leubecker, Assistant Director of National Intelligence and Intelligence Community Chief Information Officer (Acting) on 16 Dec 2010. This ICS defines the IC framework for: (a) adoption of IC enterprise standards best-suited for achieving the DNI goals of interoperability and information sharing: (b) management of an IC Enterprise Standards Baseline (ESB) consisting of minimal, focused, coordinated set of such standards; and (c) compliance and compliance certification of IC information resources and EA –related IT items with functionality relevant standards prescribed in the IC ESB.
ISO/IEC/IEEE 15026-1:2019	ISO/IEC/IEEE 15026-1:2019: Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary	(U) This document defines assurance-related terms and establishes an organized set of concepts and relationships to form a basis for shared understanding across user communities for assurance. It provides information to users of the other parts of ISO/IEC/IEEE 15026 including the combined use of multiple parts.
ISO/IEC 25000:2014	ISO/IEC 25000:2014: Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE	(U) This document provides guidance for the use of the new series of International Standards named Systems and software Quality Requirements and Evaluation (SQuaRE). The purpose of ISO/IEC 25000:2014 is to provide a general overview of SQuaRE contents, common reference models and definitions, as well as the relationship among the documents, allowing users of the Guide a good understanding of those series of standards, according to their purpose of use.
ISO/IEC 25021:2012	ISO/IEC 25021:2012: Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality measure elements	(U) This document provides guides to specify Quality Measure Elements (QME) and initial set of QME as examples. QME is a measure defined in terms of a property and the measurement method for quantifying it, including optionally the transformation by a mathematical function.

ID	Title	Description
ISO/IEC 25010:2011	ISO/IEC 25010:2011: Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models	(U) This document contains a model for data quality that is complementary to this model. The scope of the models excludes purely functional properties, but it does include functional suitability. The scope of application of the quality models includes supporting specification and evaluation of software and software-intensive computer systems from different perspectives by those associated with their acquisition, requirements, development, use, evaluation, support, maintenance, quality assurance and control, and audit.

Table 2 (U) Data Positions

5 (U) Patterns

(U) This section of the DRA outlines the use of patterns within the RAF process. Generically, patterns are models of architecture representations that provide some degree of reuse. Patterns can be represented as: viewpoints, graphical/textual models, or diagrams that show relationships between elements and artifacts specified by the principles and positions. It is important to identify the pattern and describe it with enough detail for it to be clearly understood and used appropriately.

(U) From an RA perspective, design patterns are critical for driving out data interoperability. Design patterns are a general, reusable integration solution to a commonly occurring problem within a given context of a subject area or domain. Design patterns are technology-independent and provide specific standards, positions, architectural, and other guidance on one of more occurring problems. Once completed, design patterns would be addendums attached to this document.

(U) An RA document (set of artifacts) consists of a key element called "Patterns," which is addressed at a high level in this DRA document with one or more addenda containing details about specific design patterns. RAs conform to a standard format. The DRA deviates from the standards embodied in the earlier CRA and ICAM RA documents, because the DRA reflects the most recent ODNI/IC CIO/AIG RAF process which evolves and matures over time.
(U) The DRA design patterns addenda section will be completed in a future iteration of the DRA.

6 (U) Vocabulary

6.1 (U) Vocabulary Introduction

(U) The DRA adopts the IC Data Management Lexicon (DML) as required by *ICS 501-01, IC DML, 28 October 2019,* represents a majority of the DRA vocabulary. As of March, 2021, some

DML definitions are still being debated with the IC Office of General Council (OGC). To ensure legal compliance, and in accordance with the preference expressed by the IC CDO team, the DRA is including a reference to the *ICS 501-01, IC DML, 28 October 2019*. See References section in this DRA.

- The official version of the *ICS 501-01, IC DML* is maintained on the IC CDOC ODNI Page.
- Working versions of the *ICS 501-01, IC DML* are maintained on the IC DML R-Space site.

6.2 (U) Vocabulary Process

(U) As the DRA continues to evolve, terms requiring definition or clarification will be identified and worked through the appropriate IC forums.

6.3 (U) DRA and IC DML New Terms Synchronization Process

(U) The ODNI IC CIO AIG team logs new data management-related terms, with authoritatively sourced definitions, for proposed inclusion in the IC DML and the DRA. The *ICS 501-01, IC DML* outlines the IC CDOC process and responsibilities for identifying, approving, and managing the IC DML. The identified terms will be submitted through this process for approval and inclusion in the published the *ICS 501-01, IC DML*.

6.4 (U) DRA Definitions of Data Terms

(U) Other non-DML data terms, definitions, and sources are listed in the table below.

(U) Table is Unclassified/ in its entirety

Term	Definition	Source
Data/ Information Assurance	Primarily refers to quality and integrity where 1) quality is the degree to which the characteristics of data/information satisfy stated and implied needs when used under specified conditions and 2) integrity is the degree to which a system, product, or component prevents unauthorized access to, or modification of, computer programs or data/information. This provides the grounds for justified confidence that a claim has been or will be achieved.	Derived from International Organization for Standardization (ISO)/ International Electro-technical Commission (IEC) 15026-1:2019, 25000:2014, ISO/IEC 25021:2012 & ISO/IEC 25010:2011
Domain	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.	CNSSI 4009-April 6, 2015
Fabric	A term used generally to describe an information environment that supports data at a particular security classification level.	Derived From: IC Enterprise Architecture (EA) Fiscal Year (FY) 17-18 Baseline Signed: Dec 2017
IC Information Environment (IE)	The individuals, organizations, and information technology capabilities that collect, process, or share sensitive compartmented information, or that, regardless of classification, are operated by the IC and are in whole or in majority funded by the National Intelligence Program.	ICD 121 Signed: Jan 2017
Non-Person Entity	An entity related to IT with a digital identity that acts in cyberspace but is not a human actor. This can include hardware devices, software	Derived from: CNSSI 4009-April 6, 2015

	applications, software objects (virtual/logical entities) and information artifacts.	
Pattern	Patterns are models of architecture representations at a level of generality that provides some degree of reuse. Patterns can be represented as: viewpoints, graphical/textual models, diagrams that show relationships between elements and artifacts specified by the principles and positions. It is important to identify the pattern and describe it with enough detail for it to be clearly understood and used appropriately.	DoD OASD/NII, RA Description, June 2010, Page 3-7
Reference Architecture	An authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple solution architectures, and is correspondingly influenced by multiple solution architectures.	Derived from DoD OASD/NII, RA Description, June 2010, p. 3
Reference Architecture Framework Process	A consistent, repeatable, and verifiable methodology process for driving out secure, interoperable, and enterprise-driven operational capabilities. The RAF process is designed to optimize the balance between meeting the needs of the enterprise with the autonomous requirements of IC elements.	Derived from RAF process managed by the ODNI/IC CIO/AIG organization (as of September 2020)

Table 3 (U) DRA Definitions of Data Terms

(U) APPENDIX A Glossary

Parameters	Description
Enterprise	The DRA's area of focus is the IC IE and component enterprises. An IC element may also find an RA useful for its enterprise level needs.
Consumers	The DRA supports authorized IC and non-IC consumers; consumers may be person entities (PEs), non-person entities (NPEs), or an authorized digital identity. A non-person entity is an entity with a digital identity that acts in cyberspace, but is not a human actor. This can include organizations, hardware devices, software applications, and information artifacts. [Committee on National Security Systems (CNSS) Glossary]. An authorized digital identity is a digital representation (e.g. an alphanumeric string) uniquely identifying entities (e.g. a user, process, or disk) within a system or organization which should be granted access to data.
Data Centricity	An architectural approach that results in a secure environment separating data from applications and making data available to a broad range of tools and analytics within and across security domains for enrichment and discovery. This environment embraces a more disciplined approach to intelligence integration by ensuring that data is sharable, discoverable, accessible, understandable, retrievable, and protected.
Data Quality	The degree to which data is accurate, complete, timely, consistent with all requirements and business rules, and relevant for a given use.
Discover & Access	Activities that ensure data can be found by and made available to any authorized consumer, and protected through policies for access control and need-to-know. This starts dissemination (In Accordance With [IAW] Intelligence Community Directive (ICD) 501) for data that is made accessible outside of an IC element.
Increased Information Sharing	By making both data and technology fit for purpose, the DRA enables increased information sharing through data conditioning and guiding standardized interfaces and exchanges.
Lines of Business (LoB)	The DRA focuses on supporting the intelligence operations LoB; the DRA also enables joint operations with other key LoBs including Homeland Security, law enforcement, Defense, and civilian agencies on national security measures. For the IC to have operations with law enforcement and others outside, the IC must have nation security nexus.
Master Data Management	Processes that control management of master data values to enable consistent, shared, contextual use across applications, of the most accurate, timely, and relevant version of truth about essential mission and business entities. Usually enabled by technology so that mission, business and IT work together to ensure the uniformity, accuracy, stewardship, semantic consistency and accountability of the enterprise's official shared master data assets.
Operational Modes	The DRA supports connected, disconnected, and intermittent operational domains to enable the IC IE Data Strategy's mission statement of "get the right data, to the right person, at the right time, and in the right form."
Partnerships	The DRA facilitates information sharing, increased safeguarding, and intelligence integration within the IC IE; it also fosters foreign and domestic partnerships outside the IC IE to support joint tradecraft (e.g., Five-Eyes Enterprise [5EE], DoD). In accordance with DNI/General Counsel /Management; state, local, tribal, academia, industry/private sector, and other non-Title 50 organizations should not have "joint tradecraft" with the IC since they do not have IC supported legal authorities.
Providers	The DRA supports IC providers of data capabilities (e.g., data service providers, element data stewards) as well as interoperability with non-IC providers.
Reference Data Management	Processes that control vocabularies (defined domain values), including control over standardized terms, code values and other unique identifiers, business definitions for each value, business relationships within and across domain value lists, and the consistent, shared use of accurate, timely, and relevant reference data values to categorize data.

Table 4 (U) DRA Glossary

(U) APPENDIX B Acronyms

(U) Table is Unclassified in its entirety

Acronym	Term
AIG	Architecture and Integration Group
AIM	Augmenting Intelligence using Machines
BPMN	Business Process Modeling Notation
CDO	Chief Data Officer
CFR	Code of Federal Regulation
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CLPT	Civil Liberties, Privacy, and Transparency
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CRA	Collaboration Reference Architecture
DAMA	Data Management Association
DMBOK	Data Management Body of Knowledge
DML	Data Management Lexicon
DNI	Director of National Intelligence
DoD	Department of Defense
DRA	Data Reference Architecture
E.O.	Executive Order
FY	Fiscal Year
IC	Intelligence Community
IC CDO	IC Chief Data Officer
IC CDOC	IC Chief Data Officers Council
IC CIO	IC Chief Information Officer

IC CIOC	IC Chief Information Officers Council
IC DML WG	Intelligence Community Data Management Lexicon Working Group
IC EA	Intelligence Community Enterprise Architecture
IC IE	Intelligence Community Information Environment
ICAM	Identity, Credential, and Access Management
ICAM RA	Identity, Credential, and Access Management Reference Architecture
ICD	Intelligence Community Directive
ICS	Intelligence Community Standard
IE	Information Environment
IEC	International Electro-technical Commission
ISO	International Organization for Standardization
IT	Information Technology
IC JAWG	IC Joint Architecture Working Group
LoB	Lines of Business
NIS	National Intelligence Strategy
ODNI	Office of the Director of National Intelligence
OPEN	Open, Public, Electronic and Necessary
RA	Reference Architecture
RAF	Reference Architecture Framework (Process)
PII	Personally Identifiable Information
SME	Subject Matter Expert
SQuaRE	Systems and Software Quality Requirements and Evaluation
TIC NG	Technical Integration Committee Next Generation
U.S.	United States

Table 5 (U) DRA Acronyms

(U) APPENDIX C References

A. The 1990 National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*
B. The 2017 National Security Presidential Memorandum-7, *Integration, Sharing, and Use of National Security Threat Actor Information to Protect Americans*
C. The 2018 National Security Presidential Memorandum-9, *Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise*
D. The Americans with Disabilities Act of 1990
E. Chapter 4 of title 10, United States Code, Department of Defense Authorities
F. Chapter 44 of title 50, United States Code, *National Security Act of 1947*
G. E.O. 12333, *United States Intelligence Activities*, as amended;
H. E.O. 13526, *Classified National Security Information*
I. Executive Series 00651, *Delegation of Intelligence Community Information Management Authorities and Responsibilities*
J. IC CIO Memorandum 219-003, *Information Technology and Data Asset Inventories*, 20 January 2019
K. ICD 101, *Intelligence Community Policy System*, 22 October 2019
L. ICD 113, *Functional Managers*, 19 May 2009
M. ICD 121, *Managing the Intelligence Community Information Environment*, 19 January 2017
N. ICD 122, *Services of Common Concern*, 19 July 2019
O. ICD 208, *Maximizing the Utility of Analytic Products*, 9 January 2017
P. ICD 304, *Human Intelligence*, 9 July 2009
Q. ICD 500, *Director of National Intelligence Chief Information Officer*, 7 August 2008
R. ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*, 21 January 2009
S. ICD 503, *Information Technology Systems Security Risk Management*, 21 July 2015
T. ICD 801, *Acquisition*, 16 August 2009
U. ICS 501-01, *IC Data Management Lexicon*, 28 October 2019
V. ICS 500-20, *Enterprise Standards Compliance*, 16 December 2010
W. The Intelligence Reform and Terrorism Prevention Act of 2004
X. The Open, Public, Electronic and Necessary (OPEN) Government Data Act of 2017
Y. The Privacy Act of 1974
Z. Section 2001.23, Code of Federal Regulation, *Classification Marketing in the Electronic Environment*
AA. Subchapter B of title 36, United States Code, *Records Management*