Department of Defense

Information Enterprise Architecture (DoD IEA)

Version 2.0

Volume II – IEA Description

July 2012

Prepared by:

Department of Defense

Office of the Chief Information Officer

(This page intentionally left blank)

EXECUTIVE SUMMARY

In the face of numerous, varied, and complex Information sharing challenges facing the Department, the DoD CIO has set a vision to deliver an Information Enterprise (IE) that enables DoD and partners to securely access information and services they need at the time, place and on approved devices of their choosing. To achieve this vision the DoD CIO is leading a new unifying initiative called the Joint Information Environment (JIE) focused on five major focus areas which are driven by and aligned to Joint requirements. The DoD IEA v2.0 is the authoritative capstone architecture that describes priority areas, principles and rules, and activities that guide the evolution of the DoD IE to realize the JIE vision.

The five major focus areas of the JIE will be delivered incrementally with increasing optimization of information, network, hardware, applications and governance. The JIE is focused on delivery of IT infrastructure that compliments warfighting and mission capabilities. Four of the initial focus areas that deliver capabilities are Data Center Consolidation, Network Normalization, Identity and Access Management (IdAM), Enterprise Services, all within a single Security Architecture. Each of these focus areas will have a reference architecture that leverages the content from the DoD IEA v2.0.

The value of the DoD IEA is that it provides a clear, concise description of what the DoD IE must be and how its elements should work together to accomplish such a transformation and deliver effective and efficient information and service sharing. Information is viewed as a strategic asset throughout the Department and includes everything along the continuum from data to knowledge. The DoD IEA enables proper planning for shaping the DoD IT landscape, managing the acquisition of required resources, and effectively operating the resulting IT environment. The DoD IEA describes a future vision for the JIE based on merging mission operational needs with the concepts previously embedded in separate net-centric strategies. It is subdivided into a manageable set of required capabilities which are discrete actions the DoD IE must either perform or provide. Each of these capabilities is described in terms of activities, services, and rules necessary to ensure the capability is achieved. The DoD IEA outlines how capabilities are delivered by providing descriptions of services the DoD IE must have to operate at optimum effectiveness. These services represent a collection of required information across the spectrum of Doctrine, Organization, Training, Material, Leadership and education, Personnel, Facilities, and Policy (DOTMLPF-P).

The capability descriptions allow the development of a transition plan to evolve from the current DoD IE to the future vision of JIE. A common view and understanding of the DoD IE enables stakeholders to determine their path for IT transformation and develop and direct a unified approach to achieve that transformation across the Department by providing the basis for

acquisition decisions, portfolio assembly and implementation, and planning, programming, and budget execution.

Major stakeholders of the DoD IEA are: architects, investment decision-makers, and program managers. Architects use the DoD IEA's content and structured view of what the DoD IE must be and how it must operate to develop Reference Architectures (RAs). These RAs provide the necessary level of technical direction and standards to direct development of standardized, interoperable or consistent solutions across the Department. They are incorporated into the DoD IEA as extensions of the requirements. Architects also use the content of the DOD IEA and approved RAs to develop Mission Area, Component, and solution architectures able to drive JIE-conformant solutions. Investment decision-makers use the descriptions of required DoD IE capabilities as a baseline to determine where existing and projected capabilities will not achieve the DoD IE vision. They then determine how to spend available funds to fill identified gaps. Program managers use the DoD IE capability descriptions to design programs and then measure their progress towards achieving desired capabilities as described in their Information Support Plans (ISP). They also use the rules associated with capability descriptions to guide and test program abilities.

The DoD IEA is the authoritative source for DoD CIO-designated architecture governance bodies to determine compliance with the IE vision in achieving mission effectiveness, cyber security, and efficiency goals. Strategic planners and policy writers must incorporate DoD IEA content during development of their documents. Compliance guidance is provided in various sections of the DoD IEA as described below.

For ease of use, DoD IEA v2.0 has been divided into the following:

- Volume I – a managerial and key decision-maker overview of the DoD IEA v2.0
- Volume II – an architect compendium on the DoD IEA v2.0 architectural description and, appendices on use of (Appendix D) and compliance with the DoD IEA v2.0 (Appendix E) and compliance with the DoD Enterprise Architecture (DOD EA) (Appendix G)
- DoD IEA Information Reference Resource (I2R2) Tool – search and understand the relationships of policy, guidance and other authoritative documents with DOD IEA v2.0 capabilities/services

In today's information environment the DoD IEA rules apply within the persistently-connected Internet Protocol (IP) boundaries of the Global Information Grid (GIG). Outside of these boundaries, the principles still should be considered, but the rules of the DoD IEA must yield to the state of technology, and the needs and imperatives of the Department's missions.

Table of Contents

(This page intentionally left blank)

Introduction for the DoD IEA v2.0

1 Overview of the DoD IEA v2.0

The DoD Information Enterprise Architecture (DoD IEA) is the authoritative capstone architecture that sets the operational context and vision of the Information Enterprise (IE). It addresses the concepts, strategies, goals and objectives related to the IE and provides a common, enterprise foundation to guide and inform IT planning, investment, acquisition and operational decisions in achieving the IE vision. It describes the IE capabilities that enable DoD operations by establishing the activities, rules and services involved in providing the IE capabilities. In order to oversee the DoD transition to the IE vision, the DoD IEA v2.0 has provided enhanced compliance criteria. The DoD IEA enables alignment of DoD architectures with the IE vision, drives enterprise solutions, promotes consistency throughout the DoD IE and complements the IT Enterprise Strategy and Roadmap (ITESR).

The DoD IEA v2.0 is a continuation of the effort within the DoD CIO to describe the evolving IE concepts and strategic positions. Previous versions of the DoD IEA were priority area based descriptions of the IE. The initial version (v1.0) identified five priority areas to focus near-term decision making and established a baseline framework of principles and rules to guide investments in these areas. Later updates (v1.1 and v1.2) described how to apply the principles, rules, and associated activities; criteria for DoD IEA compliance; and provided DoD Enterprise Architecture (EA) compliance requirements. The DoD IEA v2.0 describes the vision for the future IE and the initial set of capabilities it must provide to enable DoD Mission Area and Component operations. The DoD IEA v2.0 focuses primarily on warfighter operational requirements that include a smaller set of operational requirements that are common across all Mission Areas and Components. It was also developed using information from existing sources with differing purposes, scopes, and perspectives. The continued evolution of the DoD IEA will enhance the capabilities to address unique mission area and component requirements; refine and better focus the activities, rules, functions, and services used to achieve the IE capabilities; and increase the level of detail and analysis to further support IT investment decision making and solution development for the IE.

To accommodate operational needs, the DoD IEA v2.0 has evolved to a capability based description of the DoD IEA. It incorporates content from the Global Information Grid (GIG) 2.0 Operational Reference Architecture (ORA); clarifies the IE vision; introduces required IE capabilities described through activities, rules, services, and standards; and continues to institutionalize this content. The capabilities described in the DoD IEA v2.0 align closely with the Net-Centric Joint Capability Area (JCA). Incorporation of the GIG 2.0 ORA results in more comprehensive activity decompositions and an operational context that describes the operational concepts, characteristics, and requirements that drive the future IE. The GIG 2.0 ORA also addresses the day-to-day operations of the Department that are relevant to business and intelligence operations.

Enterprise-wide Reference Architectures (RAs) play a key role in extending the DoD IEA and providing more detailed information to guide and constrain solutions and implementations for a specific focus area. These RAs, along with general DoD IEA information, provide the basis for

compliance with the DoD IEA. A content navigation support tool, referred to as the IEA Information Reference Resource (I2R2) is also being developed to accompany the DoD IEA v2.0. The I2R2 consolidates and organizes compliance and guidance information by document type, capability type, and other categories to help understand compliance and analysis.

Future increments of the DoD IEA will continue to enhance and refine content, as necessary, to describe changing enterprise strategies and priorities; update relationships, application, and use; and clarify compliance criteria.

1.1 Purpose

The purpose of the DoD IEA v2.0 is to provide a strategic level architecture to stakeholders. The DoD IEA will be extended with detail by developing reference architectures. The content of the IEA and the RAs will be provided in formats supporting different stakeholder needs, done through a set of tools that will promote the use of the IEA and RA content for decision-making. The DoD IEA impacts IT efficiencies by:

- Establishing the authoritative vision for the DoD IE
- Providing the technical enterprise direction necessary to implement the DoD IE vision
- Providing context and guidance to critical Department-wide efforts such as the IT Enterprise Strategy and Roadmap (ITESR) and the IT Effectiveness effort
- Providing prescriptive architectural content for DoD IE compliance processes and tools
- Providing direction to IT stakeholders in formats supporting their needs through a set of tools that promote IE content-based decision-making

1.2 Goals

The DoD IEA v2.0 provides a means to ensure that all applicable DoD programs, regardless of Component or portfolio, align with the DoD IE vision and enable agile, collaborative net-centric information sharing. The goals of the DoD IEA v2.0 are to:

- Provide the basis for an IE that better enables Warfighting, Business, and Defense Intelligence domain operations
- Provide a traceable line-of-sight from strategic guidance to solution architectures
- Provide direction for proper planning for transforming the DoD IT landscape
- Enable more informed acquisition of resources
- Effectively operate the resulting IT environment

In achieving these goals, it is necessary to describe and institutionalize the capabilities and services required to meet operational requirements. To do this, the DoD IEA must provide information and descriptions, useable in analysis, that answer stakeholder questions.

1.3 Scope

The DoD IEA v2.0 expands, enhances, and evolves the description of the future IE and supports DoD IT investment decisions based upon tiered accountability and federation considerations.

The Department's approach to net-centric transformation in this environment is guided by the concepts of Tiered Accountability and Federation. Tiered Accountability aligns responsibility for decision making and execution across the Department. Federation ensures decision makers and implementers understand and align programs and capabilities horizontally and vertically across all these levels. A federated approach allows each element (in accordance with its Title authority) to leverage the decisions and services of other elements. Each element governs the areas, for which it is responsible, and should acknowledge and maintain consistency with guidance from higher level reference architectures. To improve understanding, Department architectures depict department-wide rules and constraints while Component architectures depict mission-specific services and capabilities and Solution architectures depict solutions that conform to higher rules and constraints. The following areas are described in the DoD IEA v2.0:

- Operational context for the IE
- A traceable line-of-sight from strategic guidance to solution architectures.
- IE vision and the capabilities needed to achieve the vision
- Activities, rules, services, and standards for providing the IE capabilities
- Refined compliance criteria for the DoD IEA

These descriptions are provided through a robust set of architecture views including All Views (AV), Capability Views (CV), Operational Views (OV), Service Views (SvcV), and Standards Views (StdV). The DoD IEA informs and constrains enterprise-wide decisions that influence the requirements for systems and solutions with a focus on the following three primary sets of customers:

a. Architects: Includes architects across capability portfolios, Federal Agencies and DoD Components. They use the DoD IEA in the development of architectures to align touch points and boundaries, as well as to identify interoperability gaps and the requirements for federation. DoD architectures, including the DoD IEA, are collectively known as the federated DoD Enterprise Architecture (DoD EA). This means that DoD Architectures are autonomous, but they apply common services, processes, and standards to ensure interoperability. The components of the DoD EA include strategic guidance such as policy; the DoD Architecture Framework (DoDAF); the OMB FEA reference models; tools such as repositories and registries; and the set of federated Command/Service/ Agency (C/S/A) enterprise, reference, and solution architectures.

b. Investment Decision Makers: Includes Investment Review Boards (IRBs), Capability Portfolio Managers (CPMs), CIOs, and others managing IT investments. In addition to providing investment criteria, architecture information can help identify key business processes to enable with a solution, and help determine whether to deliver capability via enterprise-wide services or with Component-specific services. This will enable investment decision makers to comply with the tenets of DoDD 8000.01, such as:

- Measure IT investments against the desired IE end state vision
- Analyze, select, control, and evaluate IT investments based on DoD IEA v2.0 requirements
- Assess and manage IT investment risks via DoD IEA v2.0 analysis
- Review IT investments for conformance with DoD IEA v2.0, its associated reference architectures, and the IT standards and related policy requirements included in them.
- Use DoD IEA capabilities and services and their associated principles, rules and standards to ensure interoperability and information assurance requirements will be met through investment portfolio strategies and decisions

c. Program Managers: Includes DoD and Component Program Executive Officers (PEOs), Program Managers (PMs), and their functional requirements managers. The DoD IEA v2.0 translates and clarifies operational requirements and strategic guidance into a coherent, easy to understand, and actionable set of capability descriptions to serve as the basis for acquisition and budget planning, implementation development, and program development and execution. PMs use the description of the IE vision and the resulting capabilities, services, activities and pertinent principles and rules to ensure compliance with the DoD IEA v2.0. They use the line of sight provided by both the architecture views and the documents in the I2R2 to make decisions for fielding capabilities and developing reference architectures that provide greater detail. These stakeholders ensure compliance by assessing their programs to determine whether:

- IT solutions are based on IE capabilities and services and adhere to the principles, rules, policies and standards associated with those capabilities and services
- IT solutions solve a specific part of an overall mission problem and deliver a measurable benefit and use the operational requirements associated with the IE capabilities and services and their associated principles, rules, policies and standards in determining benefits.
- Pilots and prototypes for large, high-risk IT solutions use the DoD IEA v2.0 requirements to ensure desired objectives and prototypes are achieved in accordance with the IE end state vision

The parts of the DoD IEA v2.0 that are most applicable to program managers and acquisition planners are Sections 3 through 7 and Appendices B, D, and E of Volume II and the I2R2 web based tool.

Enterprise-wide RAs are a key component of the DoD IEA because they provide more detailed content on capabilities, as well as rules, patterns, and technical positions for specific IE focus areas. DoD IEA v2.0 also provides an information navigation support tool referred to as the I2R2. The vision, principles, and rules in the DoD IEA support the DoD's war fighting, business, and intelligence missions. Evolution of the capabilities based on this architecture must recognize

and navigate obstacles at the tactical edge, such as constraints in bandwidth, information latency, and emissions control. Certain rules are not fully achievable in an Emission Control environment as network Public Key Infrastructure (PKI) authentication requires two-way communication. Similarly, in many Battlespace systems milliseconds matter; however, many state-of-the-art Internet Protocol (IP) and SOA-based technologies operate in seconds, not milliseconds. Architectures don't trump the laws of physics, the state of technology, or operational needs of commanders in the field.

In today's information environment the DoD IEA rules clearly apply within persistently-connected IP boundaries of the GIG. Outside these boundaries, the principles still should be considered, but the rules of the DoD IEA must yield to the state of technology, and the needs and imperatives of the Department's missions.

DoD IEA provides context to help everyone from policy makers to system developers understand implications of principles and business rules. Applied pragmatically, the DoD IEA will drive common solutions and promote consistency and integration across DoD's key programs, applications, and services.

Figure Intro1.3-1, DoD IEA Concept Map, illustrates the scope of the DoD IEA. Using the DoD IEA as a central organizing document for aligning the parts of the IE is critical. The definitions provided below Figure 1.3-1 allow navigation through the concepts in the DoD IEA Concept Map to increase the understanding of each component in relation to other components.

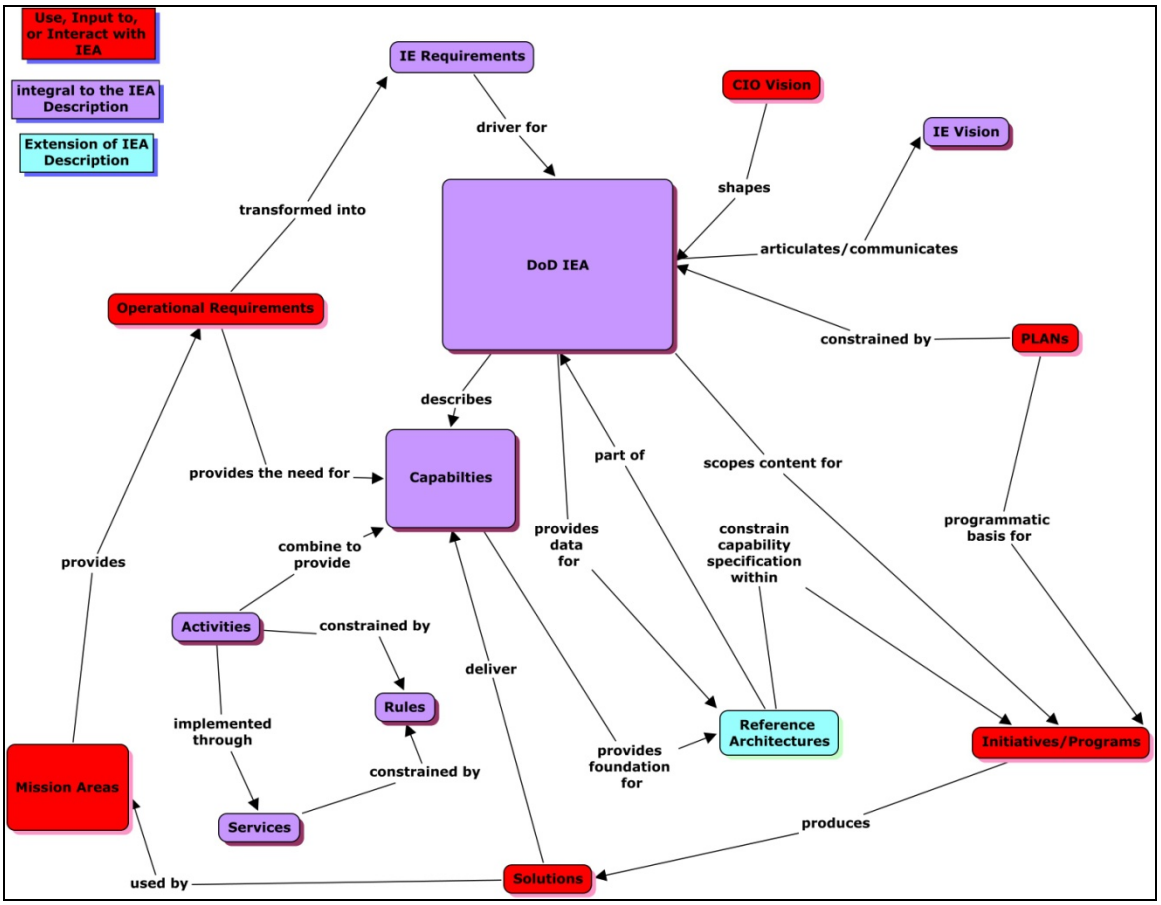


Figure Intro1.3-1 - DoD IEA Concept Map

- The ***Mission Areas*** (Warfighting, Business, Intelligence, and Enterprise Information Environment) provide warfighting ***Operational Requirements***. The fulfillment of successful operations is measured against those requirements.
- The warfighting ***Operational Requirements*** are transformed into **IE Requirements** that the Enterprise Information Environment ***Mission Area*** must provide in order to facilitate meeting warfighting ***Operational Requirements.*** The warfighting ***Operational Requirements*** are also the justification for the need for ***Capabilities*** from the IE.
- The consolidated set of ***IE Requirements*** becomes the driver for defining the IE and is the foundation of the ***DoD IEA.***
- In addition, the vision for the future IE (the ***CIO Vision***) shapes the content of the IE and the resultant documentation of that vision in the ***DoD IEA***. The result is that the ***DoD IEA*** captures that vision and the evolution of the IE is managed through the ***DoD IEA.***
- There are several ways of organizing the ***IE Requirements***. Based on the desire to aggregate ***IE Requirements*** by separation of concerns and acquisition utility (i.e., alignment with the JCIDS Capabilities-Based Assessment [CBA] approach to acquisition), the organizing principle was to use ***Capabilities*** to define packages of ***IE***

Requirements. See Note[1] for further discussion on the meaning of ***Capabilities*** in the context of the IE.

- ***Capabilities*** are described through ***Activities*** that are performed. The alignment of independent operational ***Activities*** to IE ***Capabilities*** provides users of the DoD IEA with an understanding of the ***Activities*** that need to be performed to enable that capability and the fact that some ***Activities*** are needed by multiple ***Capabilities***.
- The ***Activities*** are the basis for defining the scope of what ***Services*** need be implemented to meet the ***IE Requirements.*** As noted previously, ***Activities*** are developed independently of ***Capabilities*** to optimize their use and reuse by one or more ***Capabilities.***
- The alignment of ***Services*** to each IE capability provides users of the DoD IEA with a better understanding of the resources and associated processes needed to achieve each capability. This alignment is accomplished through associating ***Services*** with ***Activities*** that are required of, and implemented through, those ***Services.***
- The alignment of principles and ***Rules*** to IE ***Capabilities*** provides users of the ***DoD IEA*** with a better understanding of constraints that have been imposed on achieving each capability. The alignment is accomplished through associating ***Rules*** with ***Activities*** and, subsequently, to ***Services.***
- An important activity for the CIO is to specify, based on common enterprise-wide services and improved interoperability, Enterprise-wide ***Reference Architectures***. CIO prescription or DoD Component ***Solution*** Provider needs for greater detail or guidance is the basis for the development of needed Enterprise-wide ***Reference Architectures*** that provide greater architectural detail for specific areas of the DoD IEA. Many times, ***Reference Architectures*** are organized around a capability or combination of ***Capabilities*** that are needed in the IE. Once the ***Reference Architecture*** is developed and approved it is considered a part of the ***DoD IEA*** and provides more detailed architectural content for application and compliance in relevant architectures**.**
- Under the direction of the DoD CIO, Strategic ***Plans*** for implementation of ***Capabilities*** are developed for evolution of the IE.
- Strategic ***Plans*** are the basis for ***Initiatives/Programs.*** In order to influence or prescribe how the ***IE Requirements*** are implemented in ***Solutions*** (i.e., constrain the capability specification)***, Reference Architectures*** may be directed as part of an ***Initiative/Program.***
- The ***Initiative/Program,*** authorized by approved ***Plans,*** provides the programmatic direction for the development/production of ***Solutions.***
- The ***Solutions*** are developed to meet mission needs in accordance with the IE guidance where applicable.

[1] The current formal definition of a "capability" is: the ability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks [Chairman of the Joint Chiefs of Staff Instruction/Manual (CJCSI/M) 3010 series]. In the context of the IEA, we define ***IE Capability*** **as the ability to achieve an objective (goal) in support of a military operation (mission) using the Information Enterprise (IE)**. As such, the "objective" is represented as a description of a set of aggregated requirements around a stakeholder concern.

2 DoD IEA Document Organization

The DoD IEA is organized into two separate volumes. Volume I is a management overview of the DoD IEA that focuses on general content, the value of the content, and intended uses for the content. Volume I is useful for all readers, but specifically targets those readers that should use the DoD IEA in the execution of their duties. Volume II is a description of the DOD IEA providing more detailed information about the architecture views and results of architecture analysis. Its target audience is architects and other readers that require greater detail about the DOD IEA to perform their duties. Volume II also contains a set of appendices providing additional information that is relevant to all users, including information for applying and complying with the DoD IEA.

(This page intentionally left blank)

Volume II – Architecture Description

1 Introduction

Volume II provides detailed information about the architecture descriptions for the DoD IEA v2.0. It is primarily intended for architects and others that require detailed architecture information about the development, management, operation, and use of the IE. Volume II is written to be understood on its own; however, reading Volume I first gives the reader general information about the IEA and its uses that will greatly improve the understanding and appreciation of Volume II.

The DoD IEA must provide information and descriptions, useable in analysis, that answer specific questions. **Table 1-1** contains the questions that must be answered and a reference to where information answering that question can be found in Volume II.

Table 1-1 - Stakeholder Questions Answered by the DoD IEA

Questions to be Answered	Related Information in Volume II
What is the end-state vision for the IE?	Section 4
What are the metrics for measuring progress in achieving the end-state IE?	Appendix E
What end-user capabilities are provided by the IE?	Section 5
What capabilities are needed to secure and defend, operate, manage, and govern the IE?	Section 5
What activities, rules, functions, and services are associated with each capability?	Section 9
What are the compliance requirements for the DoD IEA v2.0?	Appendix E
How does information in the DoD IEA v2.0 assist stakeholders from an investment planning and implementation perspective?	Section 1 and Appendix D
How are the DoD Mission Areas and DoD Components associated with the DoD IE?	Sections 1 and 2
How does the DoD manage and operate the IE to ensure it is available and ready for use?	Sections 4, 6, and 7 and Appendix B-Shared Infrastructure Environment principles and rules
How does the DoD ensure the communications/computing infrastructure is adequate for supporting global net-centric operations?	Sections 4, 6, and 7 and Appendix B-Shared Infrastructure Environment/Computing Infrastructure Readiness/Communications Readiness principles and rules
How does the DoD ensure that information resources are secure, trusted, and accessible across the entire DoD network environment?	Sections 4, 6, and 7 and Appendix B-Secured Availability principles and rules

Questions to be Answered	Related Information in Volume II
How does the DoD enable the creation and deployment of data, information and services in a net-centric environment?	Sections 4, 6, and 7 and Appendix B-Data and Services Deployment principles and rules

1.1 Understanding Key Terms

Using terms and language that are commonly understood is, and will always be, a challenge in developing strategic architectures and their description documents. A variety of terms have been used over time to define architectural documentation at both the component and enterprise levels of the DoD. This can cause problems in communicating the intent of the various enterprise architecture artifacts and documents across the enterprise if the meanings of key terms are not established up front. Key terms and definitions are provided in Appendix A, Acronyms and Glossary.

1.2 Document Organization

This document is organized in a manner that will assist the reader in understanding the content of and relationships among the architecture descriptions. It also contains a set of appendices that further assist all stakeholders in understanding, applying, and complying with DoD IEA content. Architecture descriptions are presented in an order that logically flows from operational requirements through a vision for the end-state of the IE, to a more detailed description of the required capabilities and their attributes, and finally the plans for the future. The document is organized as follows:

Section 1 - Introduction: Informs the reader about the need for this document, its content basis, and its intended use. It discusses how to use this document, defines some key terms for consistent use, describes how the various Viewpoints described in this document are related, and provides a general overview of the document.

Section 2 - Operational Requirements Basis: Describes the Operational Context and requirements that drive the IE. Primarily focuses on the incorporation of the GIG 2.0 ORA into the DoD IEA. Includes a description of operational outcomes and the operational rules derived from the GIG 2.0 ORA.

Section 3 - Operational Activity Description: Describes the operational activity node tree decomposition (OV-5a) for the DoD IEAv2.0.

Section 4 - Vision for the IE: Describes the DoD CIO vision for the IE and the delivery of IE Capabilities (CV-1).

Section 5 - Required IE Capabilities: Provides the Capability Taxonomy for the IE. Describes the capabilities the IE must provide for end-users and the enabling capabilities needed to deliver these end-user capabilities (CV-2).

Section 6 - IE Concept of Operations: Describes the high-level concept of operations for the IE. This section identifies the key components of the IE and general relationships among the components (OV-1).

Section 7 - Services Viewpoint: Provides and discusses the services context description showing the relationship of the IE enterprise services and sub-services to capabilities and service implementation programs (SvcV-1). It also provides and discusses the enterprise services and sub-services for the IE (SvcV-4).

Section 8 - Standards Viewpoint: This is a compilation of the derived Standards Views of the IE (StdV-1 and StdV-2). These are determined through linkage back to the translation of IE requirements that must be supported by the implemented services in the IE.

Section 9 - Linkage of Activities, Services, Rules to Capabilities: Summarizes the types of relationships that exist between Viewpoints. These are critical to checking the traceability of IE requirements down to the services that will be delivered to provide the Capabilities that summarize the user requirements.

Section 10 - Way Ahead: Provides the reader with insights into the work that will continue as part of this living document. It summarizes the way ahead for filling in more detailed guidance for implementation of the IE.

Appendix A - Acronyms and Glossary: Provides a list of the acronyms and terms with definitions used throughout the DoD IEA v2.0.

Appendix B - DoD IEA Principles and Business Rules: Provides a list of the DoD IEA principles and rules.

Appendix C - Operational Activity Decomposition Tree (OV-5a): Provides activity decompositions for the DoD IEA v2.0 down to the third level.

Appendix D - Applying the DoD IEA: Describes a process for applying the content of the DoD IEA v2.0 in architecture development and use.

Appendix E - Compliance with the DoD IEA: Describes the criteria for complying with the DoD IEA and provides a checklist for compliance.

Appendix F - Alignment of GIG 2.0 ORA and DoD IEA v1.2 Activities with DoD IEA v2.0 Activities: Provides a mapping of GIG 2.0 ORA v1.5 activities and DoD IEA v1.2 activities to the DoD IEA v2.0 activities; serves as a bridge to assist in transitioning to the DoD IEA v2.0.

Appendix G - DoD Enterprise Architecture Compliance Requirements: Describes the requirements for complying with the DoD EA. Guidance on Compliance Requirements for the DoD EA does not currently exist in any authoritative documents. It is included in the DoD IEA

to provide EA focused context for the IEA. This content will be captured in appropriate Policy once it is developed.

Appendix H - Detailed IE Operational Requirements: A full definition of the five core characteristics and associated desired operational outcomes that are the operator requirements for the IE.

Appendix I – Use Case (Illustrative) Examples of IEA Support to Selected Stakeholders: Provides stakeholders with example use cases showing how the DoD IEA could be used in key situations.

Appendix J – AV-2 Integrated Dictionary: Provides the architecture definitions for capabilities, activities, and services.

1.3 DoD Enterprise Architecture Context for the DoD IEA

The information enterprise is developed in the overall context of the DoD EA. A conceptual view of the DoD EA is shown in **Figure 1.3-1**. The DoD EA consists of artifacts that help describe the DoD Enterprise and assist in managing and governing that enterprise. The EA is a representation of the needs of all stakeholders for accomplishing their mission imperatives. It consists of architectures across the DoD, organized by Component-unique architectures (e.g., for the Air Force this might include both AF enterprise architectures and program-level architectures) and enterprise-wide architectures (e.g., the DoD IEA, capability architectures). Note how the DoD IEA is a cross cutting architecture that serves and informs the capabilities of the information enterprise needed by the JCAs that span the entirety of the mission capabilities provided to the warfighter. These architectures may be integrated at some level or federated to some level. The DoD EA also consists of tools for managing and capturing architectures, reference models, technical standards, architecture description guidance (i.e., DoDAF), as well as applicable laws, regulations, and policy from sources internal and external to the DoD. All of this represents what the EA is and how it will be described, as well as the elements of the EA that are realized; in totality these represent the elements of an EA Program that steers the evolution of the enterprise. All of this now directly impacts requirements for the IEA as it is described here.

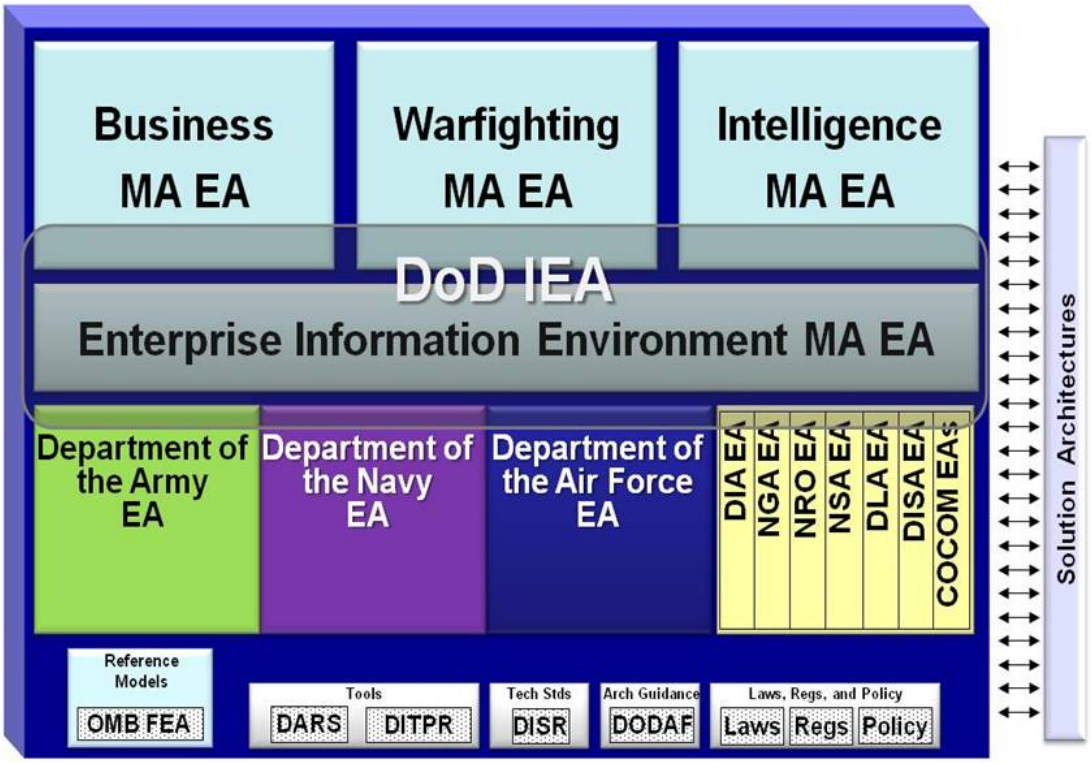


Figure 1.3-1 – DoD Enterprise Architecture

The vision for the net-centric future is for the Mission Areas that span the DoD (i.e.,Warfighting, Business, Defense Intelligence, and Enterprise Information Environment) to be provided with a robust, common, secure, agile information enterprise providing the infrastructure to facilitate information sharing anywhere and anytime; from headquarters to the edge. The IEA must meet the challenge of providing a flexible approach to developing and implementing a reference architecture for the IE while the DoD is evolving to adapt to the new realities it must meet as it moves forward. More reliance on the use of a common set of capabilities to be provided through a joint information infrastructure will provide greater effectiveness and efficiency in executing the net-centric vision for the IE.

The EIE MA and the DoD IEA have a unique relationship. The EIE represents the physical infrastructure portion of the IE and the DoD IEA is the architecture that describes the IE. In describing the IE, the IEA also describes the EIE. Therefore, it can be said that the DoD IEA is not only the architecture for the IE, but also the EIE.

Use of the IEA provides the foundation from which to make decisions on the transition as it incrementally moves toward the vision given the realities of budget, time, and resource constraints. The IEA provides a foundation that interprets the principles and rules by which the stakeholders have chosen to guide the enterprise while converting that interpretation into solid guidance on how to implement that vision. A series of architecture artifacts is documented to help answer the stakeholders' questions. By using the information from the artifacts and other associated information (e.g., financial, mission related, time related, etc.), decision makers and their staff can create stakeholder-unique, decision-focused information valuable for decision making and tradeoff analysis.

1.4 Structure of the DoD IEA

The IEA is an integrated model that helps describe the architecture from different perspectives depicted as views. These views are selected queries on the information model in a form of interest to a particular stakeholder. An important concept for the architect to visualize is how the progression of IEA related artifacts (made up of architecture "views" and other documents) from strategic to tactical information, provide important context for understanding dependencies in an integrated model of the IEA. A few definitions at this point will help the reader to better understand how to leverage this information. **Figure 1.4-1**, IEA Document Concept Map, provides a broad view of the scope of the IE that is organized around IE Capabilities. The section locations of descriptions for each of these architectural artifacts are annotated in the diagram.

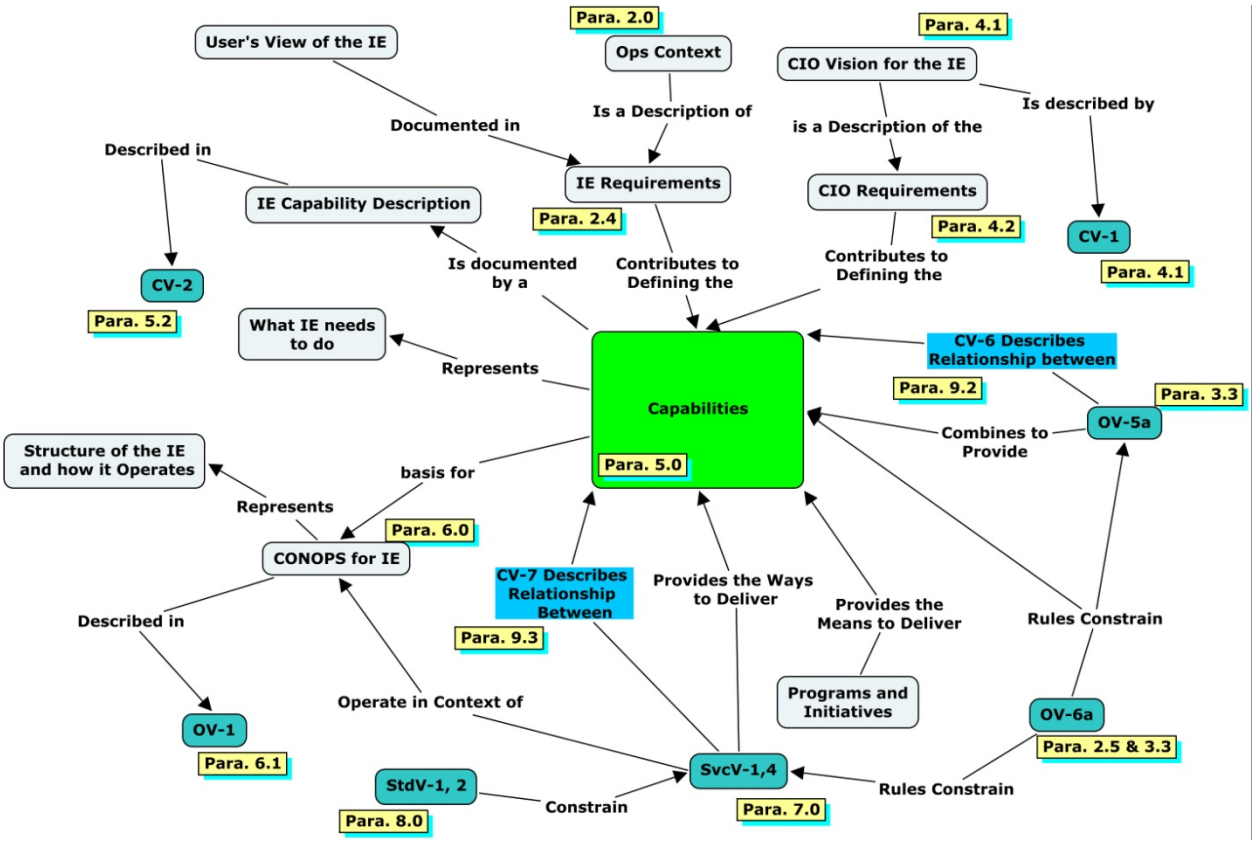


Figure 1.4-1 IEA Document Concept Map

The following is a walkthrough of the landscape of the IEA described in Figure 1.4-1:

- The ***Mission Areas*** (Warfighting, Business, Intelligence, and Enterprise Information Environment) provide warfighting ***Operational Requirements***. The fulfillment of successful operations is measured against those requirements. The Operational Requirements are transformed into requirements that an Enterprise Information Environment Mission Area must provide in order to facilitate meeting Operational Requirements. These transformed requirements become a description of the ***IE Requirements*** (i.e., the User's View of the IE). The Operational Context assists in describing the IE requirements as well. In combination the ***IE Requirements*** address the static functions that when combined in different ways will depict the expected dynamic operational behavior of the IE.
- The ***IE Requirements*** contributes to defining the ***Capabilities***. The other major contributing component is the development of ***CIO Requirements. CIO Vision for the IE*** (***CV-1*** view) represents a description of the ***CIO requirements*** (i.e., the DoD CIO Strategic Plan) for the IE. In summary, the drivers for describing the requirements for the IE are the ***IE Requirements*** and the ***CIO requirements.*** Thus the merged set of categorized requirements describes "what the IE needs to do" and is called the ***Capabilities***.

- There are several ways of organizing the requirements for the IE. Based on alignment with previous categorizations using ***Capabilities*** for the IE, and the desire to aggregate a set of requirements functionality by separation of concerns and acquisition utility (i.e., alignment with the JCIDS CBA approach to acquisition), the organizing principle was to use ***Capabilities*** to define packages of the merged set of requirements**.** See Note[2] for further discussion on the meaning of ***Capabilities*** in the context of the IE. The ***Capabilities*** are described through an ***IE Capability Description*** (***CV-2*** view***)***.
- An important element for verifying the dynamic behavior of the IE is the development of the ***Concept of Operations (CONOPS)*** for the IE**.** The CONOPS describes the structure of the IE and how it operates and is described in the ***OV-1*** view. The Capabilities (and its constituent set of Activities) is the basis for describing the ***CONOPS.***
- ***Capabilities*** are described through Activities (***OV-5a*** view) that are performed. The alignment of independent operational Activities to IE ***Capabilities*** (described in ***CV-6*** view) provides users of the DoD IEA with an understanding of the combined ***Activities*** that need to be combined to be performed to enable that capability and the fact that some of these Activities may be needed by multiple ***Capabilities***.
- ***Services (***described in the ***SvcV-1 & SvcV-4*** views***)*** provide the ways to deliver ***Capabilities***; this relationship is captured in the ***CV-7*** view. ***Services*** are constrained by applicable standards (depicted in the ***StdV-1, StdV-2*** views). In addition, the ***Services*** operate in the context of the ***CONOPS***.
- The alignment of ***Services*** to each IE capability provides users of the DoD IEA with a better understanding of the resources and associated processes needed to achieve each capability.
- The alignment of principles and ***Rules*** to IE ***Capabilities*** provides users of the DoD IEA with a better understanding of constraints that have been imposed on achieving each capability. This alignment is realized through associating ***Rules*** (***OV-6a*** view), or constraints, with ***Activities*** as well as ***Services.***
- An important activity for the CIO is to specify, based on common enterprise-wide services and improved interoperability, Reference Architectures. Based on CIO prescription or DoD Component Solution Providers needs for greater detail or guidance, the basis for the development of needed Reference Architectures can be derived from DoD IEA architectural data. Many times, Reference Architectures are organized around a capability or combination of ***Capabilities*** that are needed in the IE. Once the Reference Architecture is developed and approved it becomes a part of the DoD IEA**.**
- Under the direction of the DoD CIO, Strategic Plans for implementation of ***Capabilities*** are developed for evolution of the IE.
- Strategic Plans are the basis for ***Initiatives/Programs*** initiated by the DoD CIO**.** In order to influence or prescribe (i.e., constrain the capability specification) how the IE ***Capabilities*** are implemented in solutions, Reference Architectures may be directed as

[2] The current formal definition of a "capability" is: the ability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks [CJCSI/M 3010 series]. In the context of the IEA, we define ***Capability*** **as the ability to achieve an objective (goal) in support of a military operation (mission) using the Information Enterprise (IE)**. As such, the "objective" is represented as a description of a set of aggregated requirements around a stakeholder concern.

part of an ***Initiative/Program.*** The ***Initiative/Program,*** authorized by approved Plans**,** provides the programmatic direction for the development/production of Solutions**.**

The Line-of-Sight depiction (**Figure 1.4-2**) is a hierarchy of architecture information that is inextricably related both vertically and horizontally. The vertical alignment of laterally linked and dependent architectural concepts start with DoD CIO strategy documentation and Mission Area Capability analysis synthesized into a consistent and consolidated set of Capabilities (that is the "requirements" for capabilities at this point) for the IE. Also, remember that Capabilities include Doctrine, Organization, Training, Material, Personnel, Leadership and education, Facilities, and Policy (DOTMPLF-P) impacts.

In order to provide the Capabilities, a set of activities are identified that, when executed, will provide the outcomes the Capabilities define. Activities are defined and described that provide the ability to perform the Capabilities. The definition of the activities at this point define the combined scope of people, process, and technology needed to perform the activities, without specifying the required level of hardware or software. Once the hardware and software needed to realize the capability is determined, the rest of DOTMPLF-P can be specified and accounted for in "delivery" of the service. This translation occurs through the definition of System and/or Service functions that allow specification of components that are assignable to services and influenced by technology (i.e., COTS or developed capabilities).

The description of those activities can be converted into a specification of functions that services can accomplish and that form the basis for an eventual conversion into a Service Oriented Architecture (SOA) providing the "delivered" capabilities. The services are designed into Solutions which deliver the IE Capabilities.

The Delivered Capabilities are a reflection of the IE Requirements established at the beginning of this process. It should be noted that the IE Delivered Capabilities need to deliver DOTMPLF elements of the Solution, not only the hardware and software being developed for the IE. The degree of automation of services will come from the DOTMPLF-P analysis results.

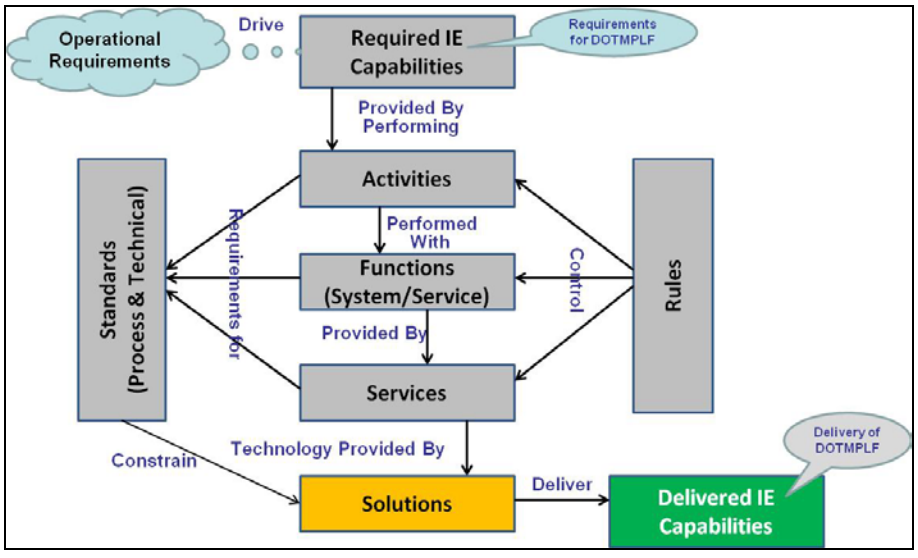


Figure 1.4-2 IEA Capabilities Line-of-Sight

The lateral relationships in the Line-of-Sight depiction need to be applied in an appropriate manner to add value to the description of the architecture. In parallel with capability development, a set of principles and rules that define the quality attributes of the IE were established and aligned with DoD CIO priorities as well as extracted from the warfighter perspective quality attributes. These rules are captured in Appendix B. Notice that the rules in Appendix B have not yet been allocated to activities, functions, and services (as shown in Figure 1.4-2); this will be accomplished in the next release of DoD IEA. The last lateral relationship shown in Figure 1.4-2 is the specification of Standards that are applied to any of the elements of the architecture that provide requirements for Solutions. Standards can be applied to processes as well as technology, and would be applied at the appropriate level of specification depending on the element of the architecture to which they apply. Ultimately, the Standards constrain the development of Solutions for the benefit of the IE. This completes the specification of both the functionality and attributes of the services to be realized in the IE.

An adjunct to this Line-of Sight is the development of Reference Architectures that complement the core of the IEA, but are an integral part of guidance derived out of the IEA. A template for determining the type of information that should be considered for a reference architecture description is provided on the DoD CIO IEA website *http://dodcio.defense.gov/Portals/0/Documents/DIEA/Ref_Archi_Description_Final_v1_18Jun10.pdf*. The scope and number of reference architectures to develop are indeterminate at this time, but an approach is suggested here that would be appropriate for maximum benefit to standardizing how the IE will develop its components in a common, integrated, and interoperable approach for IE development. The discovery of what RAs are appropriate comes from an evaluation of the priorities for capabilities planned for development. The next step is to understand the order of development based on these priorities and the dependencies of the capabilities on one another. Last is the level of specification that is appropriate to properly constrain the RAs at the level they can be used by the stakeholders for which they are intended. Such questions need to be answered by the decision makers responsible for evolution of the IE from legacy to other intermediate transition states in its evolution. The IEA does not specify the *how* here, it can only specify the *what*. It is up to managers to evaluate this discussion in the context of how they want to evolve the IE.

As seen in Figure 1.4-2, the resultant roadmap, or Line-of-Sight guidance, exists in a multidimensional space in order to properly guide the development of capabilities for the IE.

The DoD IEA presents a desired (objective) state of the IE; therefore, using the IEA as a basis for strategies to evolve the IE from its present to the future objective state is the inherent value of the IEA. Transition strategies must carefully consider the approved content of this vision document and its application to investment and technical evolution decisions in order to effectively manage and leverage enterprise-wide architecture and technology decisions that are under consideration by the DoD.

2 Operational Requirements Basis

2.1 Introduction

This section describes the operational requirements basis for the DoD IEA. It provides an overview of the required IE from the point of view of a warfighter, business, and/or defense intelligence operator and explains what the IE must be able to do to enable a user to conduct effective net-centric military operations. It presents operational requirements in the context of five core characteristics the IE must exhibit and the desired operational outcomes for each of these characteristics. It also discusses the operational rules that such requirements impose on activities, services, and capabilities implemented in the IE. In contrast, Section 6 of this Volume looks at the actual concept of operations for the IE from a more technical point of view, that of the DoD CIO, showing the technical components that comprise the IE and what those components must do to meet the operational requirements identified and described here.

The GIG 2.0 ORA converted higher-level operational requirements associated with net-centric operations across the spectrum of the JCAs into a concise description of what the warfighter needs from the information enterprise in order to successfully complete a full spectrum of assigned missions. The following subsections incorporate requirements descriptions from v1.5 of the GIG 2.0 ORA into the DoD IEA. Other viewpoints in the DoD IEA then build upon this operational context description to show how the IE should be delivered, operated, and managed to maximize its enduring value to operators as key DoD stakeholders.

To be truly representative of the needs of the DoD community as a whole, it is understood that the IEA needs to capture the detailed operational perspectives of all the Mission Areas, not just those of the warfighter. While the GIG 2.0 ORA primarily represented the point of view of the joint warfighter, it did address a large number of IE requirements common to business and defense intelligence areas as well – such things as the need for global access to the IE, the need to authenticate users prior to granting access, and user requirements for collaborating and sharing information with one another and with mission partners. Later versions of the DoD IEA will incorporate any additional and unique requirements associated with business operations, as described in the Business Enterprise Architecture (BEA), and defense intelligence operations, as described in the Defense Intelligence Information Enterprise Architecture (DI2EA). In fact, work has already begun to more closely link the DoD IEA and BEA to address unique business requirements.

2.2 Overview of Operator Requirements for IE

Achieving and maintaining an information advantage is a critical element of the strength of the United States. Information advantage is an operational advantage provided to DoD personnel and Mission Partners through optimal provision and consumption of information. To secure this advantage, the joint warfighter and enabling business and defense intelligence elements require a seamless information enterprise optimized for the tactical edge with a focus of mission assurance. This includes supporting operational functions of both advantaged and disadvantaged

users, to include external mission partners, across the full range of military operations in any operational environment, while also supporting routine, day-to-day business operations of the Department.

This information enterprise must allow all DoD elements to exercise enhanced command and control (C2) at any place and time to enable all aspects of DoD functions, in peace and wartime, from sanctuary or deployed locations. Additionally, the information enterprise must assist the interaction between the DoD and its interagency, coalition, and Non-Governmental Organization (NGO) partners by providing universal services and information supporting all operational interactions. The information enterprise must include the full range of information, resources, assets, and processes needed to achieve an information advantage and share information (which also includes the sharing of data and knowledge) across the Department and with external mission partners.

In particular, the information enterprise must meet four key objectives focused on adjusting the current "way of doing business" to a more conducive approach to defining and delivering IT capabilities and associated requirements. The following objectives are aimed at providing Theater Commanders and their support functions with the ability to address a rapidly evolving operational environment:

- Provide a unified information enterprise optimized for joint warfighter and supporting business and defense intelligence elements to facilitate force integration
- Deliver the information advantage necessary to facilitate freedom of action
- Enable secure access to required information anytime and anywhere, expediting decision cycles
- Ensure agility and versatility of the information enterprise to enable operational reach and synergy of the force

2.3 Required Operational Outcomes for IE

Achieving these objectives means overcoming existing gaps in the IE for each of the JCAs. The JCAs describe functions that must be performed to meet mission requirements and are meant to capture the complete range of DOTMLPF-P elements that must be present to perform those functions. Each JCA focuses on a specific set of required joint warfighting capabilities and associated DOTMLPF-P and is decomposed into lower-level tiers to provide more granular understanding of the specific capability requirements associated with the area.

The Joint Staff identified and analyzed deficiencies that cut across infrastructure, services, data, and policies. The analysis resulted in the determination of a set of operational outcomes representing what must be achieved to overcome these deficiencies. The operational outcomes were then grouped into the following five core characteristics for the IE, representing key

attributes the IE must exhibit to overcome identified deficiencies and enable warfighting, business, and defense intelligence missions:

- Global Authentication, Access Control, and Directory Services
- Information and Services "from the Edge"
- Joint Infrastructure
- Common Policies and Standards
- Unity of Command

Appendix H shows the operational outcomes for each of these core characteristics.

2.4 Operational Context for IE

This sub-section describes the operational context for the IE in terms of what a warfighter, business, and/or defense intelligence operator requires from the IE to enable mission success and assurance. What is described here emphasizes the Joint Staff's desire for an integrated IT infrastructure able to enhance operational capabilities of the joint warfighter, along with those business and defense intelligence support functions facilitating mission assurance and accomplishment. An IE built to these operational specifications can support all DoD, National Security, and related Intelligence Community (IC) missions and functions (strategic, operational, tactical, and business) in war and in peace, by providing the following:

- Capabilities from all operating locations including bases, posts, camps, stations, IT facilities, mobile platforms, and deployed sites
- Collaborative services within DoD and between DoD and external partners, including other Federal Departments and Communities of Interest (COIs), state and local governments, NGOs, and allied, coalition, academic, research, and business partners
- Secure, consolidated connectivity to the Internet for the purpose of conducting information sharing

Combined, achieving these joint goals will result in ubiquitous access to services by any user, from any location, on any approved (at the enterprise-level) end-user equipment. Furthermore, they serve as the foundation for managing, securing, and operating the IE.

Figure 2.4-1 provides a visual representation of the operational context for the IE. It illustrates how the five core characteristics support mission operations by providing an information environment able to achieve the desired operational outcomes, overcome identified gaps, and effectively enable net-centric operations. The diagram is an overarching view of the significant concepts, actors, and attributes of the required IE and those key relationships that should exist among these components. It is intended to promote stakeholder/user involvement in and understanding of the operational requirements for the IE; forms the basis for capturing, understanding, and analyzing the IE needs of joint warfighters in the context of the functions

they perform and the information and services they need; and allows IE stakeholders to see how they fit into the desired operational end-state. These characteristics include the important attribute of information sharing and collaboration with external mission partners.

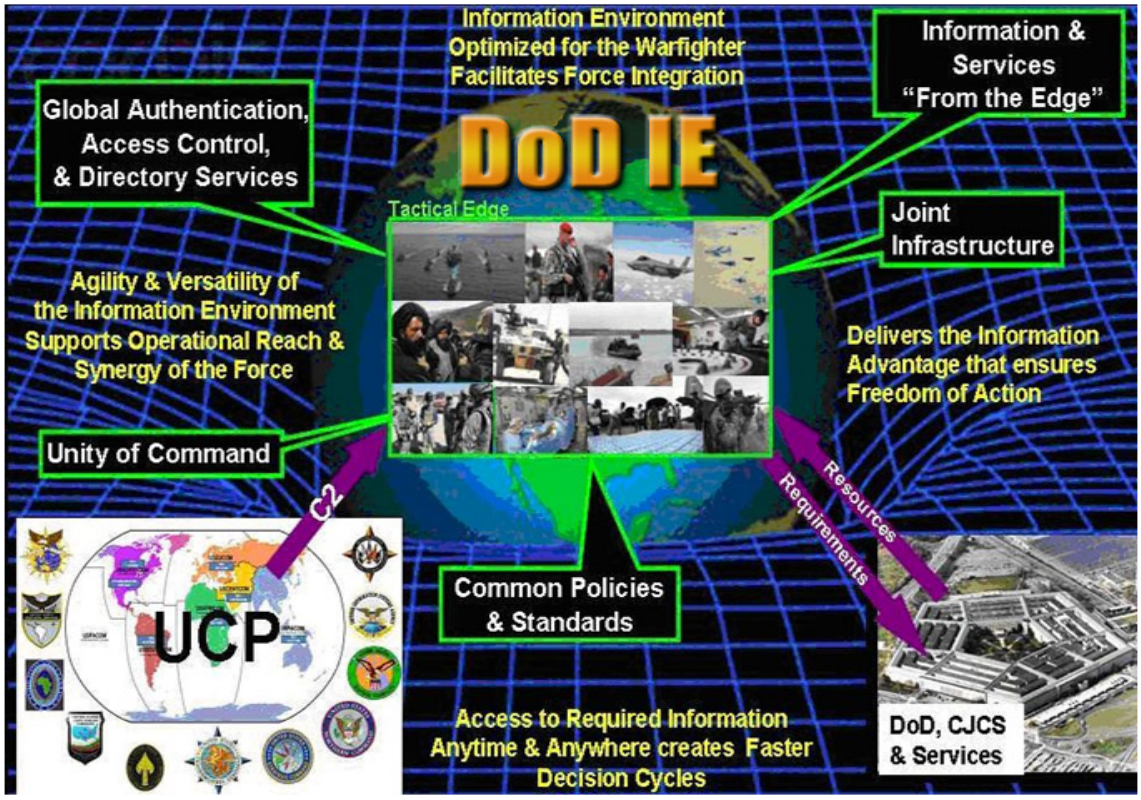


Figure 2.4-1 – Operational Context for the IE

A full definition of the core characteristics and associated desired operational outcomes can be found in Appendix H. Each subsection in Appendix H discusses, for the given characteristic, how current IT capabilities should be transformed to achieve the described end-state.

2.5 Operational Rules for the IE

As part of the analysis of the GIG 2.0 ORA, a set of rules was extracted from the desired outcomes for each core characteristic. These operational rules constrain activities, services, and capabilities described in the DoD IEA to enable the implementation of an IE able to support the projected operational environment of warfighter, business, and defense intelligence operators. The last section of Appendix B is a compilation of these rules. Section 9.1 describes how these rules align with and constrain the IE capabilities described in Section 5.0 of this document.

3 Operational Activity Description

3.1 Introduction

This section provides an overview of the operational activities that providers, users, and operators of the IE must perform to meet both operational requirements for the IE (as described in Section 2.0 of this document) and the vision of the IE (as described in Section 4.0 of this document). Specifically, performance of these activities enables an IE that can achieve the operational outcomes associated with each of the five core characteristics, defined in Appendix H, by providing user and enabling capabilities as described in Section 4.2.

3.2 Merging of Activity Models

The activity decomposition developed for this version of the DoD IEA resulted from the integration of two separate, but related, activity hierarchies. One of these hierarchies was taken from GIG 2.0 ORA v1.5, while the other came from DoD IEA v1.2.

The two activity decompositions were reconciled and it was decided to develop a functional framework in which to group activities. The key activities for the integrated activity decomposition were selected to describe actions necessary to provide an IE that can enable the core characteristics desired by joint warfighter, business, and defense intelligence operators in the context of the IE envisioned by the DoD CIO. Activities from the two source decompositions were aligned, normalized, and combined under these key new activities to form the activity hierarchy described in the next sub-section of this document.

3.3 OV-5a Description

The sub-sections that follow provide a summary of the OV-5a Operational Activity Decomposition Tree developed for this version of the DoD IEA. A more detailed description of this OV-5a can be found in Appendix C of this document.

3.3.1 Key Operational Activities

As shown in **Figure 3.3.1-1**, there are five main activities that must be performed to ensure a viable IE that meets warfighter, business, and defense intelligence operational requirements while following DoD CIO direction. These activities are part of the single parent activity A.0 **Provide the DoD Information Enterprise (IE)** - This activity allows the IE to function as one unified DoD Enterprise, creating an information advantage for our people and mission partners by providing: a rich information sharing environment in which data and services are visible, accessible, understandable, and trusted across the enterprise; and an available and protected network infrastructure that enables responsive information-centric operations using dynamic and interoperable communications and computing capabilities. The five main activities are:

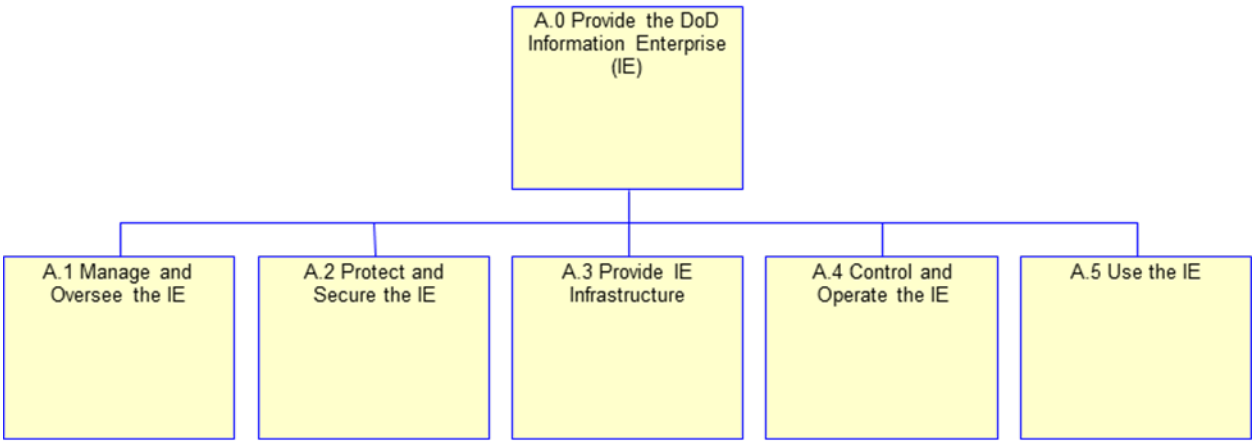


Figure 3.3.1-1 - Key Activities for DoD IEA

- **Manage and Oversee the IE** – This activity governs the development and implementation of the IE. It establishes and uses those structures and processes required to provide effective, high-level management and oversight of the components of the IE and its operations. The activity develops and enforces the required vision, strategy, and guidance to direct the IE so it meets requirements and applicable law, regulation, and policy (LRP), while at the same time delivering the capabilities necessary to fully enable net-centric warfighting, business, and defense intelligence operations for successful mission accomplishment.

- **Protect and Secure the IE** – This activity develops and implements processes and mechanisms necessary to guard critical data, capabilities, the IT infrastructure, and data exchanges within the IE, while providing authentication and non-repudiation of information and transactions to enable assurance and trust. It provides the ability to control user access to data and services, determine vulnerabilities, and prevent the exploitation of these vulnerabilities by both external and internal threats. The activity enables the monitoring of IE operations, recognition and assessment of security-related incidents, and selection and execution of appropriate responses.

- **Provide IE Infrastructure** – This activity supplies the enterprise-level communications and computing capabilities required to enable net-centric operations and the enterprise-wide services required by all users. It provides basic IT elements/components which are foundational to the DoD IE and which enable it to fully support assured information sharing across the enterprise and with mission partners.

- **Control and Operate the IE** – This activity implements capabilities required to provide integrated Network Operations (NetOps) in order to enable information access by any user across network and security domains. It includes processes and mechanisms for Enterprise Management, Content Management (which includes Records Management), and Network Defense. The activity enables NetOps to monitor the status and health and direct the actions

of DoD IE resources in support of successful accomplishment of joint warfighting, business, and defense intelligence missions.

- **Use the IE** – This activity enables an authorized user to access the IE and use its functionality to easily discover information, services, and applications, regardless of location, and to assess and critique information, services, and applications based on specific needs in order to improve IE capabilities and service. In support of operations, the activity also enables the user to collaborate and share information (which includes data and knowledge) with others.

3.3.2 Relationship of Key Activities

Figure 3.3.2-1 shows how the key activities interoperate with one another to provide an effective IE. This interaction is further described in the subsections that follow.

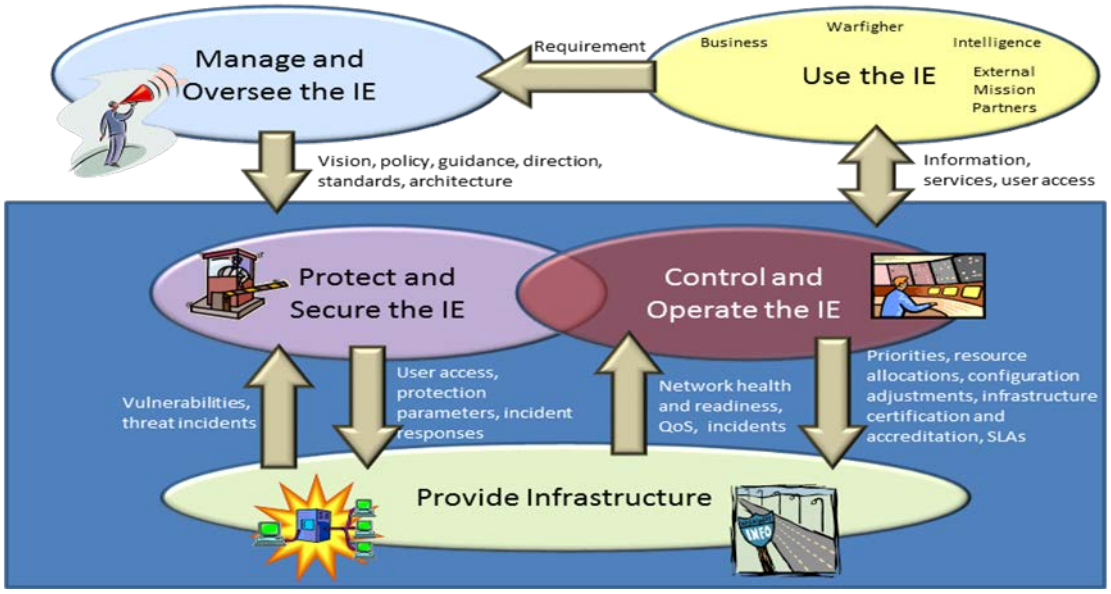


Figure 3.3.2-1 - Functional Relationship of Operational Activities in IEA

3.3.2.1 Use the IE Relationships

The ***Use the IE*** activity enables internal DoD elements and organizations performing warfighting, business, and intelligence operations and external mission partners to provide the ***Manage and Oversee the IE*** activity with their requirements for the IE. It also provides these users with access to and use of the IE to obtain the information and services needed to complete their missions.

3.3.2.2 Manage and Oversee the IE Relationships

The ***Manage and Oversee the IE*** activity turns user requirements into a vision of the IE to which to govern. This vision is architected to provide the necessary description of these requirements, how they relate, and the resources needed to meet to them. The resulting architecture data is analyzed and the results of this analysis used in developing and enforcing policies, guidance, direction, and standards to manage the protection, control, and implementation of the resources needed to deliver the vision.

3.3.2.3 Protect and Secure the IE Relationships

The ***Protect and Secure the IE*** activity takes policy, guidance, and direction from the ***Manage and Oversee the IE*** activity and works to ensure the IE is secure from both internal and external threats. It provides the mechanisms and processes to authenticate users and provide them with authorized access to and use of the infrastructure in accordance with the privileges they have been granted, while at the same time preventing unauthorized users from gaining the ability to improperly exploit the IE. The ***Protect and Secure the IE*** activity sets security parameters for infrastructure resources to minimize their vulnerability to both exploitation and attack and to prevent their unauthorized use. It enables monitoring of the IE for vulnerabilities and attempts to improperly gain access to or attack the IE and provision of the proper security incident responses. It is in this area where the ***Protect and Secure the IE*** and ***Control and Operate the IE*** activities overlap, since both enable monitoring of the IE (for different reasons) and provide appropriate responses to detected incidents.

3.3.2.4 Control and Operate the IE Relationships

The **Control and Operate the IE** activity takes policy, guidance, and direction from the ***Manage and Oversee the IE*** activity and works to ensure delivery of the IE vision through efficient and effective operation of the IE to meet rapidly and continually changing user needs. The ***Control and Operate the IE*** activity is responsible for certifying and accrediting the infrastructure in accordance with LRP so the infrastructure fully meets both user needs and those security restrictions established by the ***Protect and Secure the IE*** activity. The ***Control and Operate the IE*** activity monitors the health and readiness of IE resources and the Quality of Service (QoS) they are providing to users in accordance with negotiated Service Level Agreements (SLAs), and then adjusts infrastructure operation as necessary to deliver the best possible service. As information and service needs change in line with shifts in warfighting, business, and defense intelligence operations, this activity dynamically and proactively adjusts resource allocations and configuration of the infrastructure to ensure continual and optimal IE operations.

3.3.2.5 Provide Infrastructure Relationships

The ***Provide Infrastructure*** activity supplies internal elements and components performing warfighting, business, and defense intelligence operations and external mission partners with the means to access and use information and services needed to successfully complete their

missions, in accordance with the access granted them by the ***Protect and Secure the IE*** activity. The ***Provide Infrastructure*** activity enables and underpins the IE, providing basic communications and computing capabilities necessary for net-centric operation of the IE and those enterprise-wide services needed by all users. It provides the ***Protect and Secure the IE*** activity with information on infrastructure configuration for use in assessing vulnerabilities and threat incidents. In turn, it adopts security parameters set by the ***Protect and Secure the IE*** activity to protect infrastructure assets from exploitation and attack. The ***Provide Infrastructure*** activity is directed by the ***Control and Operate the IE*** activity to ensure effective customer service and information and service delivery. It provides information on infrastructure health and readiness, QoS, and operational incidents, and dynamically adjusts the configuration and operation of infrastructure resources to meet rapidly changing priorities and user needs.

3.3.3 Value of Operational Activities

These operational activity descriptions provide a detailed definition of all the actions required to put in place, secure, manage, operate, and use the IE to effectively enable net-centric operations and meet operational requirements. One overarching value of these activity descriptions lies in the support they provide stakeholders and users involved in planning for effective IE implementation, management, and operation. IE Planners (e.g., the DoD and Component CIOs, IE portfolio and investment managers) can compare current actions being taken to achieve the IE against these required activities to determine gaps in existing performance. IE Planners can use these identified performance gaps to measure progress in achieving the desired IE end-state by analyzing the projected results of those activities which are being performed adequately and comparing them to expected results from being able to perform all activities. In addition, activities are aligned to the required IE capabilities to show which activities are necessary to achieve each of these capabilities. By determining where gaps exist in activity performance, planners should then be able to determine which IE capabilities can and cannot be delivered to meet user needs. Using the results of these analyses, IE Planners can prioritize activity performance gaps and determine how best to assign limited resources to ensure the right activities can be executed to meet priority needs.

A second overarching value of the operational activities lies in the description of security requirements for the IE provided by the sub-activities under ***Protect and Secure the IE***. These activity descriptions provide all DoD IEA stakeholders/users with an understanding of the full set of actions that must be taken to secure information and services in the IE. The IE governance process must assess and develop policy to enforce compliance with these activities. Both IE providers and consumers must execute these activities to ensure the IE and its information remains secure in accordance with that policy and guidance. Execution of security activities must be monitored and enforced by NetOps to keep the IE secure.

A key principle in developing the activities is to ensure that they are independent of technology and focused on the enduring activities of the organization. This characteristic improves their reusability across multiple capabilities as their performance is evaluated against the purpose of

the activities. In addition, reusability is enhanced across multiple stakeholders across the DoD to assist in developing common services for improved interoperability across the enterprise.

For other stakeholders/users of the DoD IEA, the following specific areas in the activity decomposition have the following particular meaning and use:

- For those governing the IE, predominately the DoD and Component CIOs and their staffs, activity descriptions found under ***Manage and Oversee the IE*** describe specific actions that required governance processes must incorporate and that governance structures and organizations must execute in implementing those processes.

- For providers of IE infrastructure resources, to include solution architects, service developers and providers, and program managers, activities subordinate to ***Provide IE Infrastructure*** describe actions that must be taken to deliver the proper capabilities with which the solution aligns. Solution architectures should describe activities aligning with the appropriate DoD IEA activities or incorporate the appropriate DoD IEA activities to ensure solutions meet these requirements. Compliance with these activities must be enforced across DoD.

- For users of IE infrastructure resources, sub-activities under the ***Use the IE*** activity describe the actions that must be taken by consumers to effectively operate with and obtain optimal value from the IE.

4 Vision for the IE

4.1 DoD CIO Overarching Vision

The DoD CIO is tasked with improving the combat power of the Department—as well as its security and efficiency—by ensuring that the Department treats information as a strategic asset and that innovative information capabilities are available throughout all areas of DoD supporting warfighting, business, and intelligence missions. The DoD CIO Vision and Mission are:

- **Vision** - Deliver agile and secure information capabilities to enhance combat power and decision making.
- **Mission** - Information is one of our Nation's greatest sources of power. Our first and greatest goal is to deliver that power to enable the achievement of mission success in all operations of the Department including warfighting, business, and intelligence.[3]

The DoD Information Enterprise (IE), as illustrated in **Figure 4.1-1**, is the DoD information resources, assets, and processes[4] required to achieve the vision and perform the mission of the DoD CIO. A robust and seamless IE provides decision makers and action officers with

[3] Department of Defense (DoD) Chief Information Officer (CIO) Campaign Plan, baseline, Version 0, October 5, 2011, Pg. 5.
[4] DoDD 8000.01, Management of the DoD Information Enterprise, February 10, 2009, Pg. 10.

the knowledge they need to make decisions and complete actions. The DoD IE enables net-centric Warfighting, Business, and Intelligence operations as a unified DoD information enterprise. It provides a rich information sharing environment in which data and services are visible, accessible, understandable, and trusted across the enterprise. It also enables an available and protected network infrastructure that enables responsive, information-centric operations, using dynamic and interoperable communications and computing capabilities.

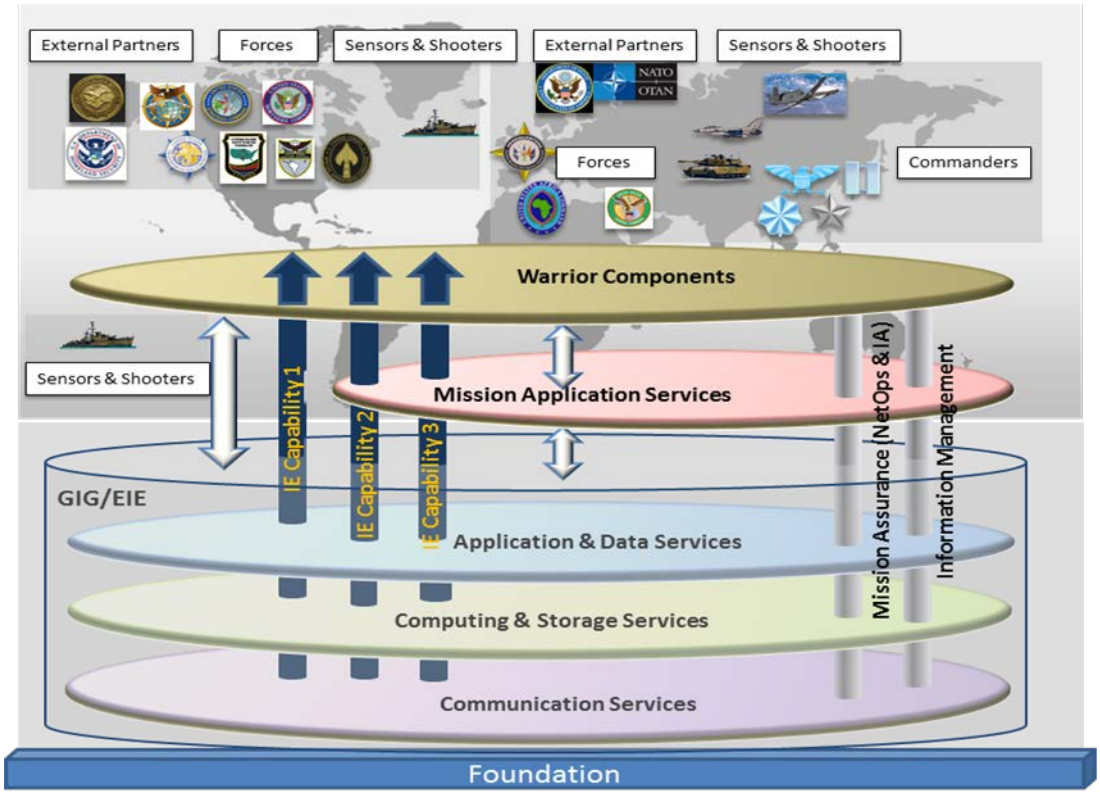


Figure 4.1-1 – Illustration of the DoD IEA

4.2 DoD CIO Vision for the IE

The DoD IE is the DoD information resources, assets, and processes[5] required to achieve the vision and perform the mission of the DoD CIO. A robust and seamless IE provides decision makers and action officers with the knowledge they need to make decisions and complete actions. The DoD IE enables net-centric warfighting, business, and intelligence operations as a unified DoD information enterprise. It provides a rich information sharing environment in which data and services are visible, accessible, understandable, and trusted across the enterprise. It also enables an available and protected network infrastructure that enables responsive, information-centric operations, using dynamic and interoperable communications and computing capabilities.

[5] DoDD 8000.01, Management of the DoD Information Enterprise, February 10, 2009, Pg. 10.

The operational requirements, described in the Operational Context[6] section as operational goals and associated outcomes, play an important role in shaping the vision for the IE. The IE must enable and support these operational requirements while also meeting DoD CIO management and oversight requirements. The IE will enable, support, and meet these requirements by:

- Providing end-user capabilities to connect to IE networks, access, and share assured information and information assets in support of achieving the operational goals and outcomes described in the Operational Context.
- Using enabling capabilities within the IE to properly operate, defend, and govern the IE in its provisioning of end-user capabilities.

Together, the end-user capabilities and enabling capabilities comprise the IE capabilities. **Figure 4.2-1,** IE Capability Vision, depicts the vision for the IE with respect to operational requirements, end-user capabilities, and enabling capabilities. The operational requirements are the basis for determining what end-user capabilities the IE must provide and are represented with the following four goals:

- Provide a unified information enterprise optimized for the joint warfighter and supporting business and defense intelligence elements to facilitate force integration
- Deliver the information advantage necessary to facilitate freedom of action
- Enable secure access to required information anytime and anywhere, expediting decision cycles
- Ensure agility and versatility of the information enterprise to enable operational reach and synergy of the force

To meet these goals, the IE needs to provide a set of capabilities that enable end-users to connect to, access, and share information and information assets in performing DoD missions and operations.

[6] The Operational Context is a part of the DoD IEA v2.0 that describes the operational requirements the IE must enable and support. These operational requirements are described as the outcomes and goals that operations must achieve.

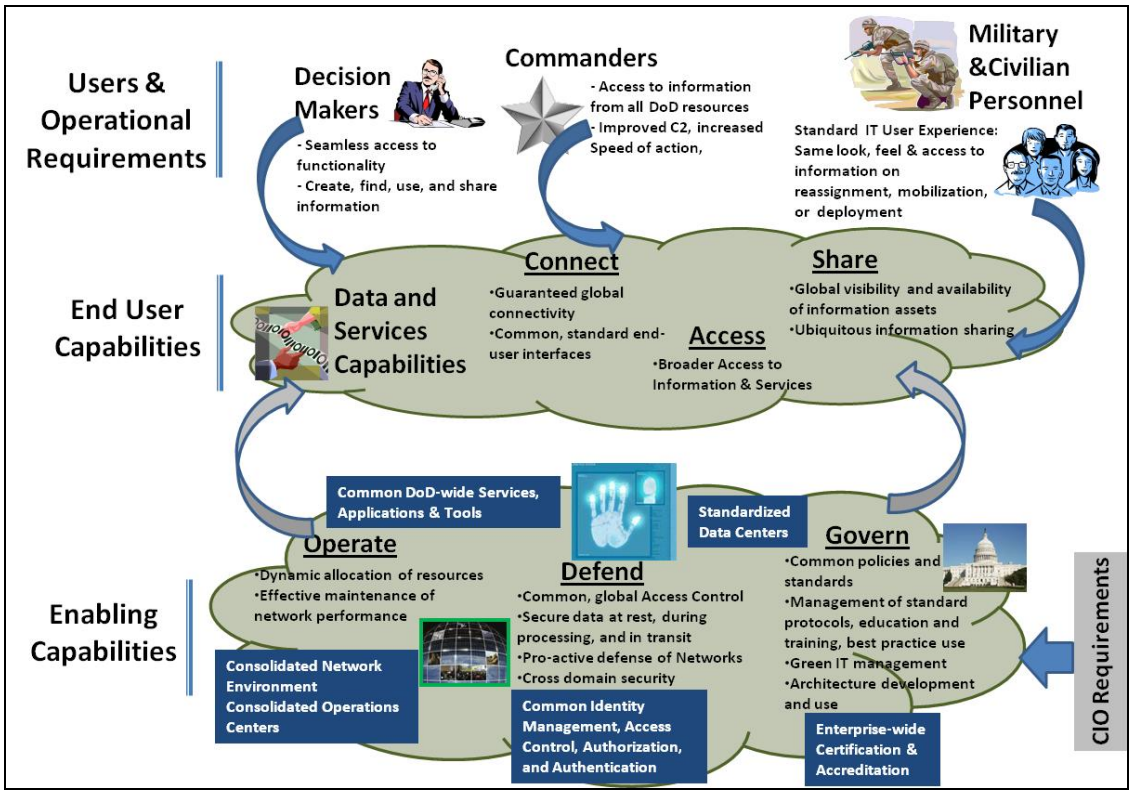


Figure 4.2-1 – IE Capability Vision

4.2.1 End-User Capabilities

End-user Capabilities enable users to perform the following:

- Connect to the IE network from anywhere, using the various end-user devices available to DoD personnel and mission partners
- Access information, services, and other information assets when needed, using the various end-user devices available to DoD personnel and mission partners
- Share information and services throughout the IE and provide global visibility and availability of information, services, and other information assets

End-user Capabilities are provided by an information infrastructure and environment consisting of Enabling Capabilities to operate, defend, and govern the IE.

4.2.2 Enabling Capabilities

The intent of End-user Capabilities is to optimize visibility, accessibility, trustability, and understandability of information by providing users simple, seamless, intuitive interaction with massive amounts of data through large-scale storage, search, retrieval, fusion and visualization capabilities. To achieve this, common processes and rules for tagging, storing, accessing, integrating, sharing, and visualizing globally distributed, heterogeneous information, data, and explicit knowledge must be established and enforced. It also requires the establishment and enforcement of policies and standards that direct common management processes and maximize information sharing. DoD CIO requirements for developing, operating and managing the IE influence the Enabling Capabilities. Together, the following Enabling Capabilities ensure:

- Effective management of network performance and dynamic allocation of enterprise resources
- Common access control for all users and devices throughout the IE
- Cross domain security and pro-active defense of networks
- Data security at all times
- Common policies, standards, and management processes
- Effective development and use of architecture

Enabling Capabilities also promote enterprise-wide, standardized operations, and resources. This includes such things as common, enterprise-wide services, applications, and tools; standardized data centers; consolidated networks and operation centers; common access control; and enterprise-wide certification and accreditation. Delivering the IE Capabilities needed to enable DoD operations requires dynamic, agile, and responsive infrastructure components. A DoD prescribed means for providing some of these enabling capabilities is through the concept and strategies for Cloud Computing.

4.3 Vision for Delivering IE Capabilities

To deliver required IE Capabilities, infrastructure components, such as computing, communications, and enterprise services resources require characteristics and attributes that enable dynamic, agile, and responsive operations. Mission Assurance, consisting of NetOps and Information Assurance, play a key role in securing and protecting the IE. Together, these infrastructure components deliver the capabilities provided by the IE. The benefits of a Cloud Computing environment are readily seen in the areas of efficiency, agility, and innovation. These benefits include:

- Improved asset utilization (server utilization > 60-70%)
- Aggregated demand and accelerated system consolidation (e.g., Federal Datacenter Consolidation initiative)
- Improved productivity in application development, application management, network, and end-user
- Purchase “as-a-Service” from trusted cloud providers
- Near-instantaneous increases and reductions in capacity
- More responsive to urgent agency needs
- Shift focus from asset ownership to service management
- Tap into private sector innovation
- Encourages entrepreneurial culture
- Better linked to emerging technologies (e.g., devices)

4.3.1 Computing Resources

The vision for computing resources is a set of consolidated and logically interconnected Core, Regional, Local and Mobile/Tactical computing centers that deliver cloud-based, on demand services to all DoD users and devices. Each computing center instantiation is operated according

to a set computing center attributes and standards for the following: dynamic allocation of resources, multi-tenant applications (server virtualization), Green IT, and the enablement of data visibility, accessibility and understandability. Computing resources of the future will:

- Enable on-demand, distributed, dynamic, and high performance computing
- Provide the ability to process data and to enable physical and virtual access to hosted information and data centers across the enterprise
- Maximize computing capacity, provide standard and well defined services optimizing assets and resources, and minimize cost in support of cross-organizational, geographically dispersed users
- Enable a service-centric IE and support new service-oriented approaches, such as cloud computing and virtualization (including IaaS, PaaS, & SaaS), for sharing, storing, processing, and transporting information
- Provide rapid and ubiquitous access to data and information anywhere on the network to authorized users (personnel or machines)
- Support dynamic, responsive Enterprise Management, Network Assurance, Content Management, and Information Assurance functions
- Be evolved such that improved processing and storage capabilities are deployed close to the "tactical edge"
- Provide a common set of foundational capabilities and services that simplify development or implementation
- Facilitate the capability to make data assets visible, accessible, and understandable.
- Provide "shared" space for data and application services
- Provide on-demand capacity and self-provisioned services that can elastically scale, as required
- Design web-based applications and services to run in consolidated and virtualized enterprise data centers as well as being "mobile device ready" from the start

4.3.2 Communications Resources

The vision for communication resources is a robust and dynamic physical and logical communications infrastructure that will accommodate ubiquitous transport of all required information and services to all authorized users. The Communications infrastructure will provide secure, agile, seamless, and survivable end-to-end connectivity (from core[7] to tactical edge) and on-demand bandwidth that is dynamically allocated, based on operational priority and precedence among the millions of space, air, sea, and terrestrial-based fixed, mobile, and moving users. The communications resources of the future will:

[7] Core refers to the Global Fixed Assets or Fixed but Mobile-in-Theater Assets.

- Contain an agile mesh of diverse landline, satellite, and wireless capabilities providing net enabled applications and data from the National Command Authority (NCA) down to the tactical edge
- Increase transport capability across the IE to accommodate emerging, net-enabled capabilities offered as services that remain readily available, secure, on-demand, 24/7
- Enable Unified Capabilities (converging IP based networked integrated applications for voice, video, and data delivered ubiquitously and over high-speed optical infrastructure) based on a unified customer interface standardized on Ethernet and IPv6 technologies
- Enable robust and extensible cross domain capabilities (capability to securely move information among multiple security enclaves) to support a secure and integrated information enterprise
- Support dynamic, responsive Enterprise Management, Network Assurance, Content Management, and Information Assurance functions
- Reduce the communications hardware footprint in the tactical environment by moving toward a single, common set of radio network components
- Be designed to allow transparency through increasingly resilient networks and flexible provisioning of net-centric infrastructure systems that are secure and highly available
- Support mobile users and mobile devices in all environments including disconnected operation, intermittent connectivity, and limited bandwidth (DIL)
- Enable virtualized and federated networks characterized by virtualized Defense Enterprise Security Architecture (DESA) Stacks which provide perimeter protection for designated regions
- Consist of a much smaller number of discreet networks than exists today achieved through consolidation and modernization initiatives now being pursued by the Military Departments (MilDeps) and other Components

4.3.3 Enterprise Services Resources

The vision for enterprise services is an agile, distributed, single service-oriented enterprise for development, management, and use of "Applications, Services, and Information" throughout the DoD enterprise. This service-oriented enterprise is more user-centric and focused on the tactical edge (i.e., end-user in garrison or deployed) by embracing simplicity, leveraging and directing current information technology investments, and aggressively seeking innovative new ways to solve the command and control issues of the Department. This vision embraces the coexistence of enterprise and mission specific services that will separately, or in combination, allow access by users to the full spectrum of services available across the DoD Enterprise. Enterprise services of the future will:

- Provide for rapid development and use of services in the IE
- Provide development environments where new services can be developed and modified/tailored for mission specific uses in the field, in near real-time

- Produce information that is easily discoverable, accessible, understandable, and useful to consumers
- Support dynamic, responsive Enterprise Management, Network Assurance, Content Management, and Information Assurance functions
- Include a common adaption layer for application services to transparently interface with enterprise infrastructure services
- Extend existing strategic applications and services to the tactical edge environment
- Provide repeatable tactical edge service implementations as well as consistent implementation results and service performance
- Improve service interoperability, reuse, and plug-n-play for new service creation
- Make services, information and capabilities seamlessly available to users in environments characterized by disconnected operation, intermittent connectivity and limited bandwidth (DIL)
- Deliver common, ubiquitous, shared services and applications as Enterprise Services freeing Components to focus on the delivery of Component-unique services

4.4 Principles and Rules for Implementation of the IE Vision

As part of the analysis of the IE Vision, a set of principles and rules were established. These principles and rules constrain activities, services, and capabilities described in the DoD IEA to enable the implementation of an IE able to support the warfighter, business, and defense intelligence Mission Areas. Appendix B is a compilation of these principles and rules. Section 9.1 describes how these rules align with and constrain the IE capabilities described in Section 5 of this document.

4.5 Summary of IE Vision

The DoD IE is essential to achieving the vision and performing the mission of the DoD CIO. The DoD IE, as a unified DoD information enterprise, creates an information advantage for our people and mission partners. It provides a rich information sharing environment in which data and services are visible, accessible, understandable, and trusted across the enterprise. It features an available and protected network infrastructure that enables responsive, information-centric operations, using dynamic and interoperable communications and computing capabilities. The DoD IE, driven by the operational requirements it must support and enable, provides a set of IE Capabilities. These capabilities consist of end-user capabilities and enabling capabilities. End-user Capabilities enable users to connect to, access, and share information and information assets in performing DoD missions and operations. Enabling Capabilities provide the ability to operate, defend, and govern the IE and comprise the information infrastructure and environment that provide End-user Capabilities. DoD CIO requirements for developing, operating and managing the IE influence and guide the Enabling Capabilities. The IE Capabilities are delivered using computing, communications, and enterprise services resources. IE Capabilities support and enable warfighting, business, and intelligence operations.

5 Required Information Enterprise Capabilities

5.1 Introduction

This section describes the IE as a collection of the specific capabilities it needs. The section converts the requirements of warfighter, business, and defense intelligence operators for information and information assets, as described in Section 2.0 of this document, into a mutually exclusive set of required IE capabilities. Each IE capability represents a unique ability required to securely consume, produce, and/or manage information and information assets within the IE. Together, these capabilities are meant to represent the totality of what the IE must be able to do or provide, as scoped by the IE Vision described in Section 3.0 of this document, to enable successful mission accomplishment. In the DoD IEA, each IE capability is represented as an architecture description of the activities, functions/services, and rules that when implemented or executed can be expected to achieve the capability in terms of a measurable result.

The value of sub-dividing the IE into capabilities in this way is that it provides decision-makers, portfolio managers, program managers, and engineers with distinct, measurable sets of requirements they can use to determine which IT solutions to implement and how those solutions should be designed and built to fully achieve actual capabilities able to meet mission needs. Because these capability descriptions have been derived from operational requirements, they can also be used to measure mission impact and risk associated with not delivering a given capability or set of capabilities. Measuring IT investments against required IE capability descriptions, then, can provide an effective way to analyze approaches for expending limited resources to enable required information sharing.

The set of required IE capabilities presented here was extracted and harmonized/normalized from an approved set of authoritative source documents. These documents included the GIG 2.0 ORA, Initial Capabilities Document (ICD), and draft Implementation Guidance; the Joint Capabilities Document for the Net-Centric Operational Environment (NCOE JCD); DoD IEA v1.2; the DoD Information Enterprise Strategic Plan 2010-2012; and the Joint Net-Centric Capability Delivery document, v0.2, dated March 2010.

5.2 Capability Description/Taxonomy (CV-2)

Figure 5.2-1 shows the CV-2 Capability Taxonomy for the IE. The required IE capabilities are shown in the diagram as yellow rectangles. Definitions of these capabilities can be found in the DoD IEA AV-2 (Integrated Dictionary) in Appendix J. In the diagram, these capabilities are organized in two tiers of capability areas, shown as blue (Tier 1) and grey (Tier 2) rounded rectangles.

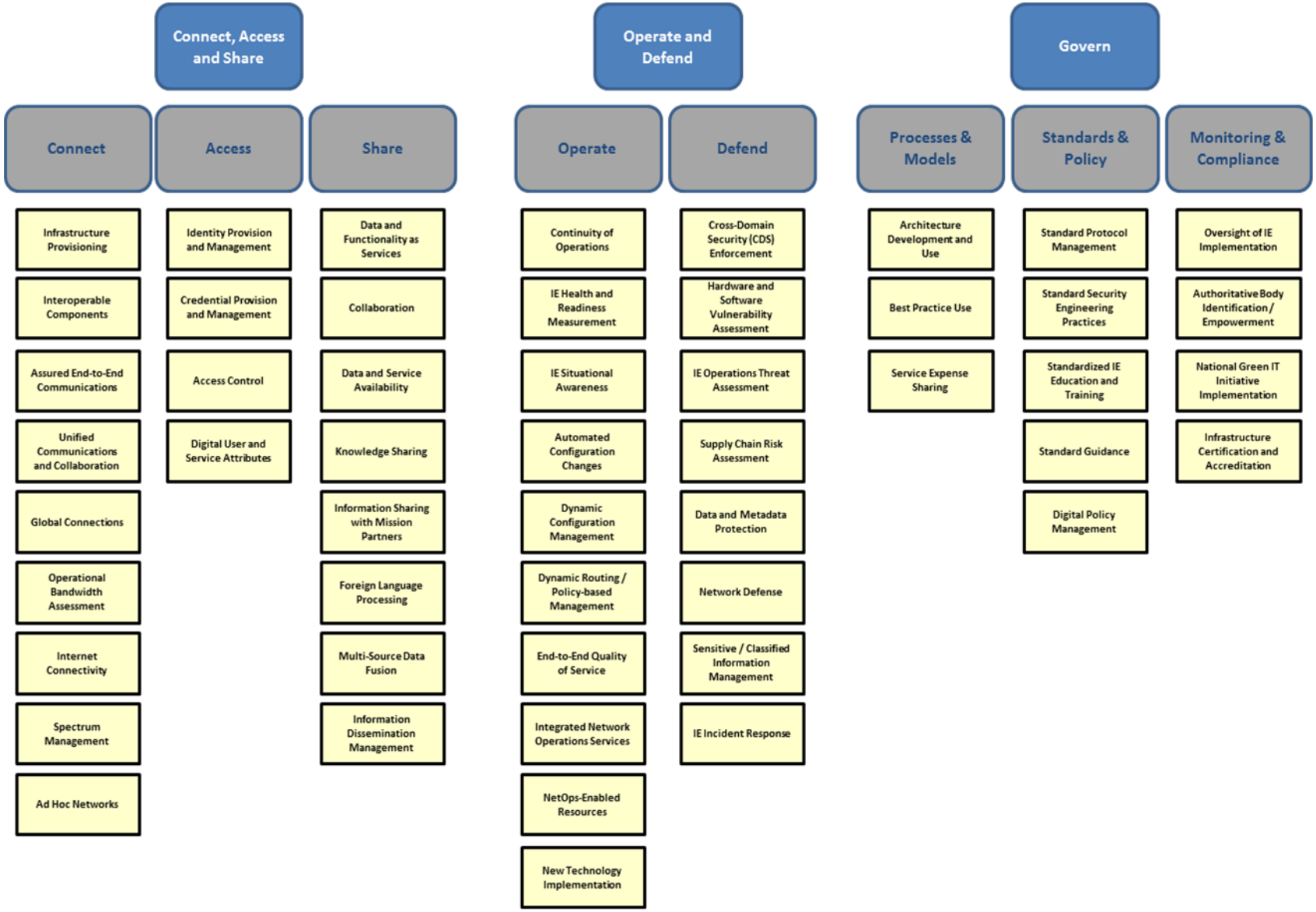


Figure 5.2-1 - IE Capability Taxonomy (CV-2)

The capability areas provide a means of grouping "like" capabilities together for analysis and planning purposes. The capability areas used in this version of the DoD IEA were chosen to reflect the structure presented in the CIO Vision for the IE (Section 3.0 of the document) and to support ease of alignment of DoD CIO Initiative and Program efforts. End-user Capabilities the IE must provide for warfighter, business, and defense intelligence operators, as described in Section 4.2.1, are grouped under the Tier 1 area Connect, Access, and Share. Enabling Capabilities that must be provided within the IE to ensure it is available for and useable by those operators, as also described in Section 4.2.2, are grouped into the other two Tier 1 areas: Operate and Defend, and Govern.

The Tier 1 capability areas are defined as follows:

- **Connect, Access, and Share** is the capability area that contains the set of capabilities enabling interoperability across Mission Areas and organizations internal and external to DoD and giving users the ability to find, access, provide, share, process, and manage information and other services.

- **Operate and Defend** is the capability area that contains the set of capabilities for managing the operation of the IE to ensure networks, services, and underlying physical assets can be dynamically allocated and configured, and data and services are secured and trusted across DoD.

- **Govern** is the capability area that contains the set of capabilities providing processes, policy and standards, and oversight of the development, deployment, use, and overall management of the IE.

These Tier 1 areas are then subdivided into Tier 2 capability areas to provide additional granularity in support of required architecture analysis and use. These Tier 2 areas are defined as follows:

- **Connect** is the capability area that contains the set of computing and communications infrastructure capabilities enabling any user or service to reach any other user or identify and use any other service.

- **Access** is the capability area that contains the set of capabilities enabling the granting or denying of available information assets to both human and machine users.

- **Share** is the capability area that contains the set of capabilities enabling information and information assets to be used within and across Mission Areas.

- **Operate** is the capability area that contains the set of capabilities providing real-time situational awareness, protection, and operational management of the IE.

- **Defend** is the capability area that contains the set of capabilities ensuring data and services are secured and trusted across DoD.

- **Processes and Models** is the capability area that contains the set of capabilities providing procedures and tools to be used for analysis enabling effective overall management of IE development, deployment, and use.

- **Standards and Policies** is the capability area that contains the set of capabilities providing patterns and strategic direction to be followed to ensure interoperability across DoD.

- **Monitoring and Compliance** is the capability area that contains the set of capabilities enabling effective oversight of development, deployment, and use of the IE.

As previously stated, each IE capability should be fully described in the DoD IEA in terms of the:

- Activities performed to enable the capability
- The services required to deliver the capability or key aspects of it, to include the functions that service needs to perform
- The rules constraining the performance of those activities, services, and functions
- The measures to determine when the desired result of the capability has been achieved

The current version of the DoD IEA describes each IE capability in terms of operational activities, principles and rules, and services. This description is further detailed in Section 9.0 of this document. Later versions of the DoD IEA will expand the capability descriptions to include the functions that need to be performed by the services to achieve the capability and the measures to determine when a capability has been achieved. In addition, future versions of the DoD IEA will align rules with the activities, functions, and services associated with each capability to better show how the rules directly constrain each of these attributes in delivering the capability.

6 IE Concept of Operations (OV-1)

The Operational Concept for the DoD IE describes the key concepts, operations, components, and participants of the IE. It provides both a user and a provider perspective.

6.1 Description of IE Concept of Operations

Figure 6.1-1, IE Operational Concept Graphic, is a graphical depiction of the IE and the operations performed within it. The upper portion of Figure 6.1-1 represents the user perspective and the bottom portion represents the provider perspective. The provider perspective focuses on the operational concept for providing IE capabilities to a user. The general Operational Concept for the IE is that user's, using various end devices, access the network, then produce and consume services and information to accomplish tasks and missions. The user's ability to access

the network, produce and consume services, information, is provided by integrating and orchestrating functionality from four IE service layers and two support areas.

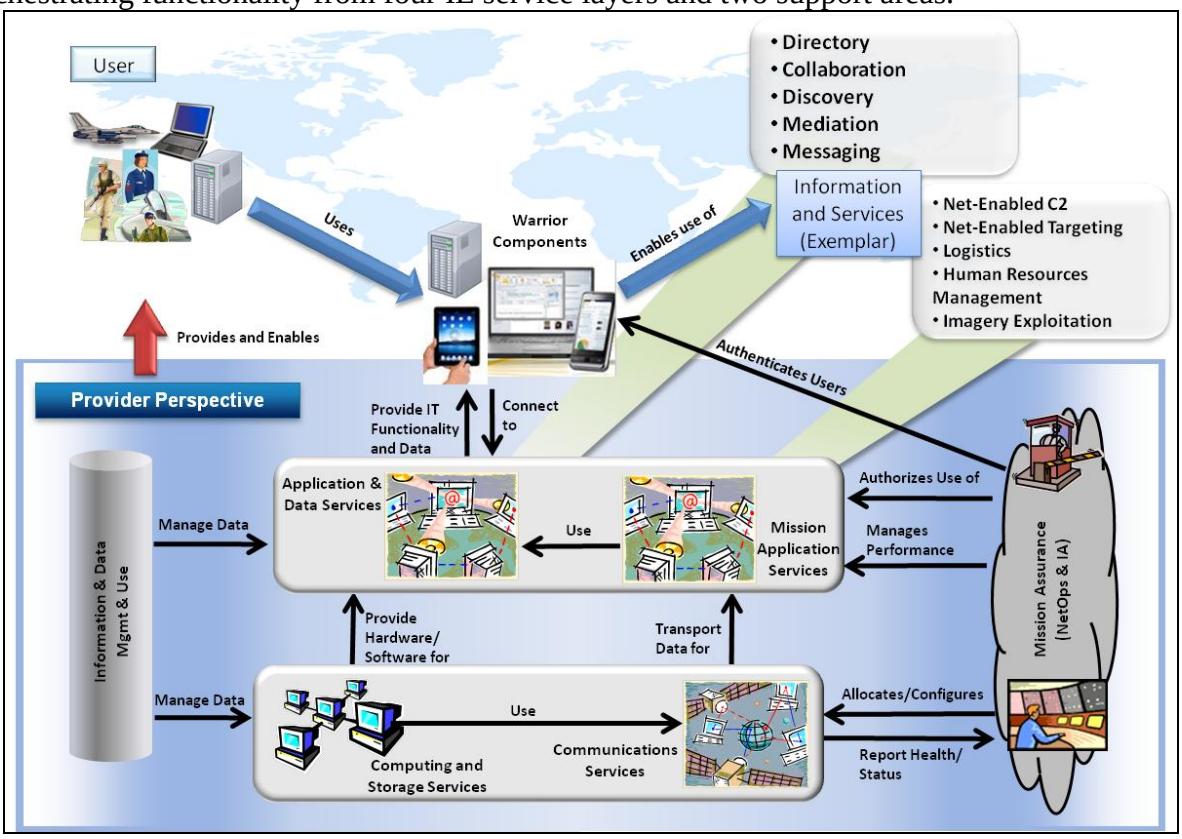


Figure 6.1-1 - IE Operational Concept Graphic

These highly automated and dynamic IE layers and support areas are:

a. IE Service Layers

1) **Communication Services** – A robust and dynamic physical and logical communications infrastructure that will accommodate ubiquitous transport of all required information and services to all authorized users.
2) **Computing & Storage Services** – A set of consolidated and logically/physically interconnected Core[8], Regional, Local and Mobile/Tactical computing centers that deliver cloud-based, on demand services to all DoD users and devices.
3) **Mission Application Services** – The set of Mission and Business services that are unique to the warfighting, business and defense intelligence Mission Areas. These services are discoverable by and accessible to authorized mission area users and are part of the service oriented enterprise.
4) **Application & Data Services** – The set of core services that are commonly used across all components of the department. These services are discoverable by and accessible to all DoD users and are part of the Service Oriented Environment (SOE).
5) **Warrior Components** – Provides the functionality to ensure user access to needed information and services through various end-user devices.

[8] Core refers to Global Fixed Assets or Fixed but Mobile-in-Theater Assets.

b. Support Areas

1) Mission Assurance

a) NetOps – The DoD-wide operational, organizational, and technical capabilities for operating and defending the GIG. NetOps includes, but is not limited to, enterprise management, net assurance, and content management. NetOps provides commanders with GIG situational awareness to make informed command and control decisions. GIG situational awareness is gained through the operational and technical integration of enterprise management and defense actions and activities across all levels of command (strategic, operational, and tactical)[9]. Includes the functions and processes performed and the organizations and technologies performing them to command and control, defend, and operate the various resources and manage information in the IE.

b) Information Assurance (IA) – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities[10]. Provides the functions needed to assure and secure information at rest, in transit, and being processed. Ensures only authorized users (including mission partners) have ready access to their information, missions continue under any cyber security situation, and associated components perform as expected and act effectively in their own defense.

2) **Information Management** – The function of managing an organization's information resources for the handling of data and information acquired by one or many different systems, individuals, and organizations in a way that optimizes access by all who have a share in that data or a right to that information[11]. Provides the functions needed to manage DoD information and data throughout its lifecycle to optimize visibility, accessibility, trustability, and understandability for all authorized users. This includes functions to comply with statutory recordkeeping requirements and further the growth of institutional knowledge and preservation of records supporting the DoD's operations and missions.

6.2 Notional Description of the Operational Concept

A notional description of a user accessing a collaboration service is used to further describe this operational concept. In this description, a DoD user accesses a collaboration service to perform tasks and missions. The operations performed to enable the user to access and use the collaboration service are described in this description.

[9] DoDI 8410.02 NetOps for the Global Information Grid (GIG).
[10] DoDD 8500.01E Information Assurance.
[11] Joint Publication 1-02 DoD Dictionary

a. All services and information are made visible and accessible to users as they are produced. Collaboration and orchestration functionality is provided by the *Application & Data Services* layer.
b. The collaboration service is made visible by properly tagging the service and posting it to an accessible storage repository provided by the *Computing & Storage Services* layer. The *Communication Services* layer provides the communications means for the computing infrastructure. Posting the service to the storage repository is accomplished using the *Communication Services* layer. At this point, the collaboration service is visible, discoverable, and accessible to authorized users.
c. A user's mobile end-user device access to the network is provided by the *Warrior Components* layer. The *Mission Assurance* (*NetOps & Information Assurance)* support area authenticates the user allowing device and network access. The *Mission Assurance* (*NetOps & Information Assurance)* support area also authorizes the user to access the collaboration service based on the user's attributes. At this point, the user has access to the collaboration service either directly or through a portal.
d. The user uses the collaboration service in the execution of tasks and missions. The information being provided and consumed is managed by the *Information Management support* area and assured and protected by the *Information Assurance* functional area.
e. At all times during the process of accessing and using the collaboration service, performance management, resource allocation and configuration, network health monitoring, and network defense functions are being performed by the *NetOps* functional area.

The operations described in this description are the same operations performed for all information and service interactions that take place in the IE. All services in the IE are provided by one or more of the service layers and support areas described in the operation concept graphic in Figure 6.1-1.

7 Services Viewpoint

The Services Viewpoint models typically describe services and their interconnections providing or supporting, DoD warfighting and business functions. Service models describe services, in part, by showing the relationships that exist within an enterprise between services and various elements contained in the architecture, such as capabilities and activities. Understanding how services directly or indirectly enable capability and operational requirements within an enterprise is critical to the successful execution of those requirements.

For the purposes of the DoD IEA v2.0, the enterprise services were developed by analyzing and rationalizing across a wide spectrum of DoD services models including Defense ITIL, GIG Enterprise Services, Enterprise-wide Access to Network and Collaboration Services (EANCS) Reference Architecture, Marine Corps Enterprise Services, and the DISA Enterprise Service Platform among others.

Services were selected for inclusion in the DoD IEA Enterprise Service Taxonomy based on the following criteria:

- The candidate enterprise service should be truly enterprise-wide. Services that are exclusively provided or managed locally, regionally, or by installation were not included in the Enterprise Service taxonomy.
- An enterprise service is defined as one that is provided by a DoD-level entity for the use by all or a large segment of the DoD user population or a service provided by a Military Department that is or can be used by other Military Departments.
- While DoDAF 2.0 services are not limited to internal system functions and can include Human Computer Interface (HCI) and Graphical User Interface (GUI) functions, for the purposes of DoD IEA v2.0 enterprise services were limited to those services which can be defined as "machine-to-machine" services. Services which are primarily consumed by people and are process driven (e.g., help deck/touch services) will be considered for inclusion in future IEA versions. This includes tasks around how enterprise services are managed and maintained.
- An enterprise service can be defined, described, and measured by service providers for purposes of inclusion in an enterprise service catalog.
- Enterprise Services should be enduring and should describe the desired functionality provided, rather than a specific implementation of that service (which will change over time). DoD service implementation programs (e.g., DISA RACE, DCO, DKO) were not included in the enterprise service taxonomy as they may change or be replaced over time. However, they have been included in the SvcV-1 and aligned to the DoD IEA enterprise services that they provide. This provides visibility to DoD service programs, some of which are required implementations of DoD IEA services, to capability developers and service providers.

7.1 Services Context Description (SvcV-1)

The services context description shows the relationship of the IE enterprise services and sub-services to capabilities and service implementation programs. While a more typical SvcV-1 might focus on how services help realize the operational requirements of the resource flows in an OV-2, the DoD IEA v2.0 development focused on providing IE operational requirements through detailed capability descriptions. Future versions of the DoD IEA may explore exchange requirements between operational activities and a new SvcV-1 will be developed at that time.

This SvcV-1 was developed to provide a context for the enterprise services in which users could understand how they enable the DoD IEA capabilities and how they are currently being realized through the existing service programs and initiatives. This fit-for-purpose model provides traceability in from each of the DoD IE enterprise services to the capabilities supported by that set of functionality. Each service is also aligned to the DoD enterprise program that provides that service. The SvcV-1 can be viewed in its entirety or by capability area for ease of viewing.

The SvcV-1 model is embedded here as an Excel document you can open by double-clicking on the icon below.

Services Context Description (SvcV-1)

7.2 Services Functionality Description (SvcV-4)

The figures in this section (**Figure 7.2-1 through 7.2-6**) show the enterprise services and sub-services for the IE. The services hierarchy starts with Tier 1 and Tier 2 services that are consistent with the capability areas. From the capability areas, services are decomposed into one or two additional tiers. For readability, the hierarchy has been broken into six different models that show the services for a capability area. Service tiers are a consistent color throughout the views so that users can differentiate between the Tier 1 and 2 service category areas (red and blue) and the Tier 3 and 4 services (green and purple). Definitions of the IE services can be found in the DoD IEA (Integrated Dictionary) in Appendix J.

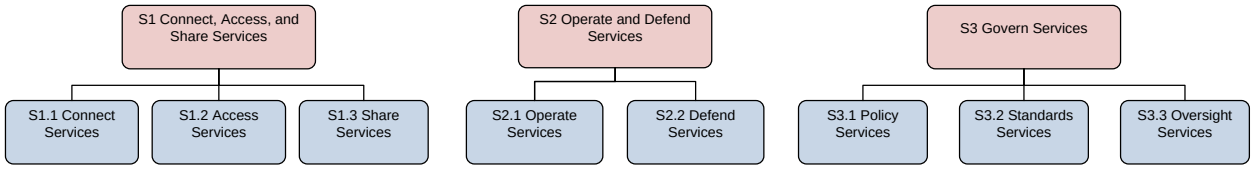


Figure 7.2-1: DoD IEA v2.0 Services Hierarchy (Tier 1/Tier 2)

As with the capability taxonomy, grouping services provides a means for "like" services to be viewed together for analysis and planning purposes. The capability areas used were chosen to reflect the structure presented in the CIO Vision for the IE (Section 4) and to support ease of alignment to on-going DoD CIO initiative and program oversight efforts. For a description and definitions of the Tier 1 and Tier 2 capability areas, see Section 5.2.

The IE services in this services hierarchy help describe the IE capabilities in the CV-2. As previously stated, the services help describe each IE capability in the DoD IEA by showing how the capability (or aspects of the capability) are delivered. This relationship also includes functions that the service needs to perform. Those functions are not explicitly defined in the DoD IEA v2.0 but are inherent in the functionality associated with each activity in the OV-5. Later versions of the DoD IEA will expand the services descriptions to include the functions that need to be assigned and performed by the services to achieve the capability and the measures which will be applied to those services. In addition, future versions of the DoD IEA will also align services to the rules that constrain how the services may be executed.

The SvcV-4 detailed model is provided as an embedded file in this document; double-click the icon below to access the PowerPoint file.

SvcV-4 Service
Context and Hierarch

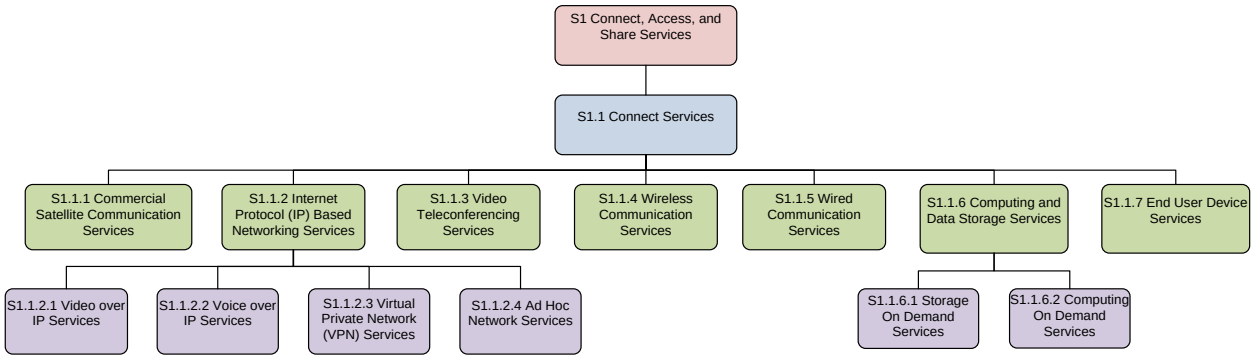


Figure 7.2-2: DoD IEA v2.0 Connect Services

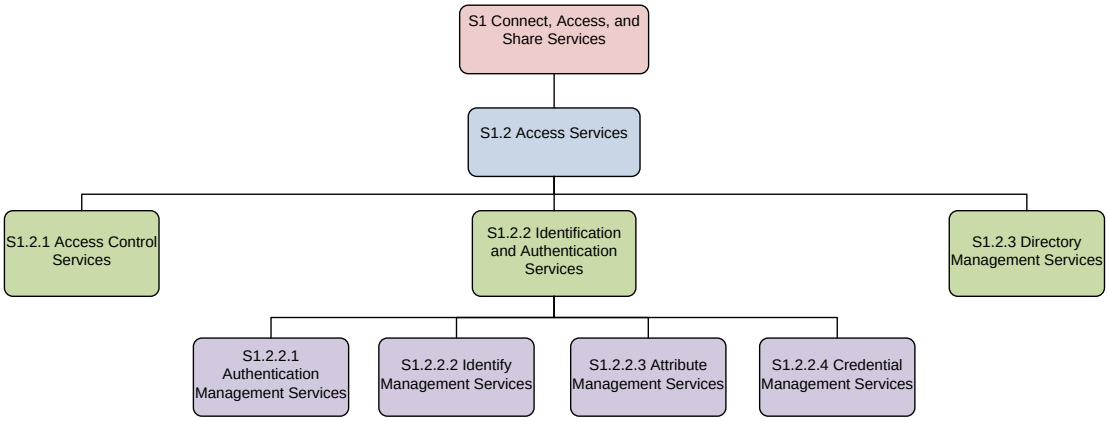


Figure 7.2-3: DoD IEA v2.0 Access Services

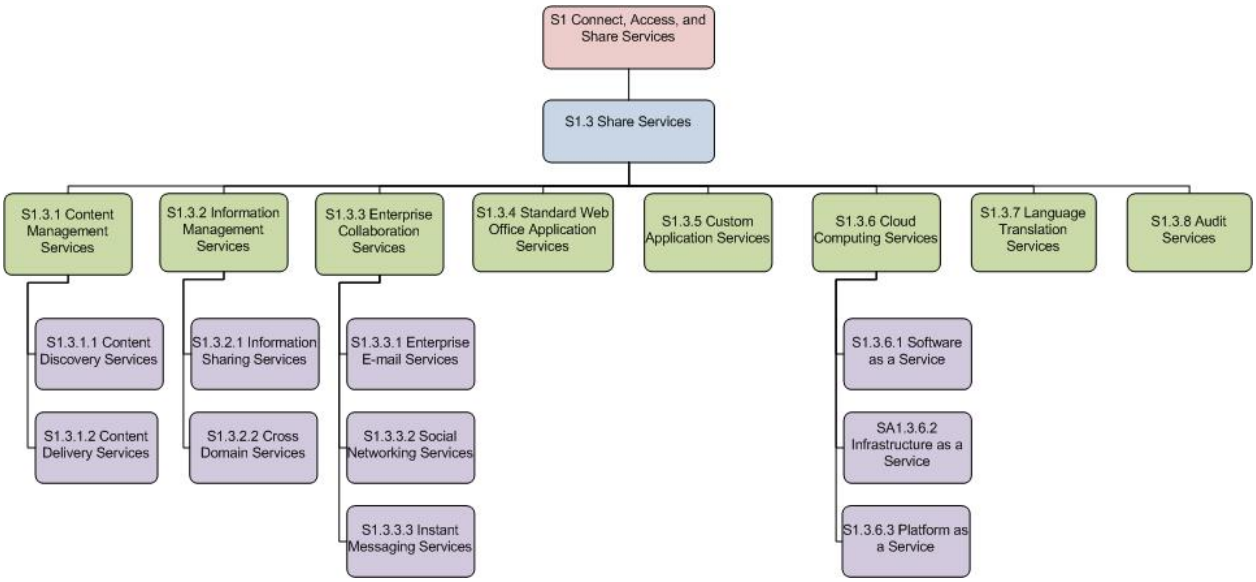


Figure 7.2-4: DoD IEA v2.0 Share Services

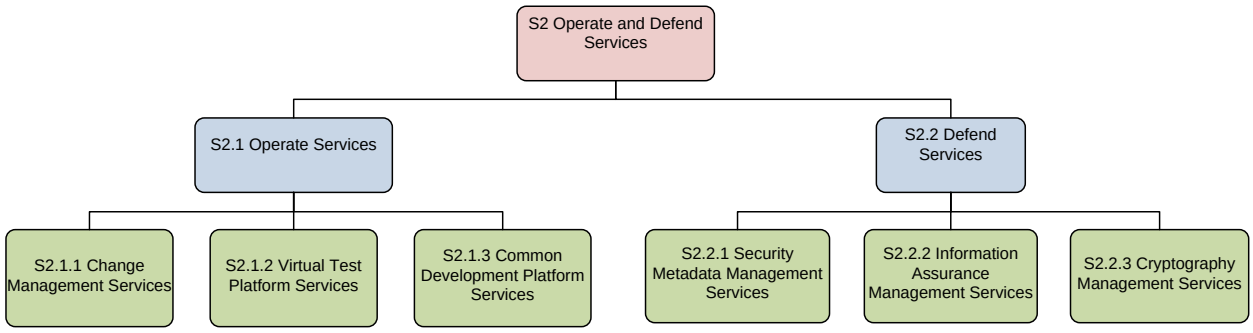


Figure7.2-5: DoD IEA v2.0 Operate and Defend Services

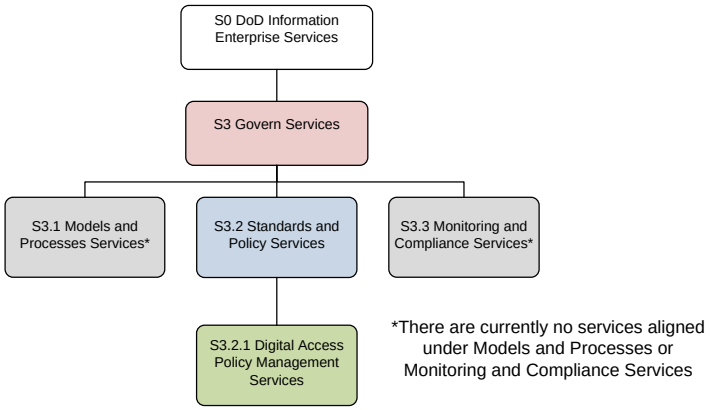


Figure 7.2.6: DoD IEA v2.0 Govern Services

8 Standards Viewpoint

8.1 Standards Profile (StdV-1)

Introduction

The DoD Information Technology Standards Repository (DISR) is the authoritative source for DoD IT standards and the DoD IEA v2.0 identifies standards that are relevant to the capabilities and services in the IEA. The purpose of a Standards Profile (StdV-1) is to define the standards, guidance, and policy applicable to the DoD IE. The Standards Profile assists the IE in identifying applicable standards, guidance, and policy by identifying and listing existing and emerging documentation containing such information. Once identified, these standards are used to direct, guide, and/or constrain the execution of capabilities or services under the IE.

Overview

This standards view (**Table 8.1-1**) is a subset of the information planned for the I2R2 and does not contain every possible standard or reference relevant to the IE. This standards view contains a list of only the documents that align to the DoD IE Architecture. For all other documents containing applicable standards, guidance, policy, and constraints, not referenced in the IE Architecture, please refer to the I2R2. The I2R2 is an example of a tool that aids in finding relevant documentation from multiple sources of content and document type.

In addition to providing a link to each of these documents, to assist stakeholders in finding standards that are applicable to their needs, the online I2R2 allows users to filter these documents by capability, service, ITESR initiative, and standard type.

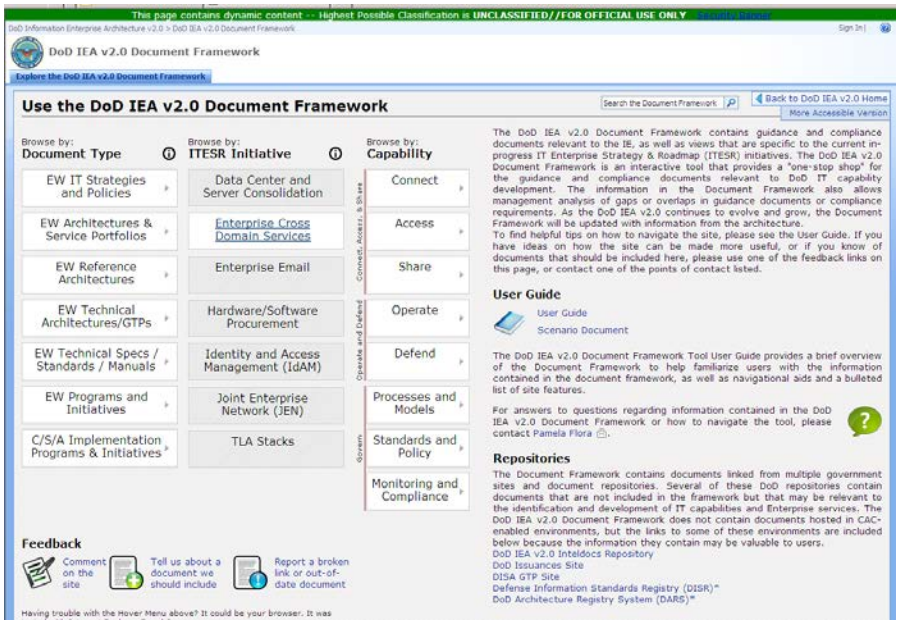
Table 8.1-1 Standards Profile (StdV-1)

8.2 Standards Forecast (StdV-2)

Introduction

The purpose of a Standards Forecast (StdV-2) is to define the standards, guidance, and policy applicable to the DoD IE. The difference between the StdV-1 and the StdV-2 is that the Standards Forecast contains only the *emerging* applicable standards, guidance, and policy. The StdV-2 (shown in **Table 8.2-1**) contains the emerging standards relevant to the capabilities, operational activities, and services contained in the DoD IEA. The purpose of the StdV-2 is to identify critical standards and the impact of these standards on the future development and maintainability of the architecture. Knowledge of emerging standards helps organizations make investment decisions and supports strategic planning. Once the standards in the StdV-2 have been approved by the appropriate governing body, these standards are moved to the Standards Profile and are considered formal compliance requirements.

The emerging standards in a StdV-2 are usually aligned to the expected availability of the emerging standards and the anticipated availability predictions are related to the elements and the time periods that are listed in the SV-8 Systems Evolution Description, SvcV-8 Services Evolution Description, SV-9 Systems Technology & Skills Forecast, and SvcV-9 Services Technology & Skills Forecast models. The set of standards in this StdV-2 are not aligned to expected availability time periods because most frequently this information was not available. Since the DoD IEA doesn't contain these planning documents, the standards contained in the StdV-2 could not align to the planning elements in an SV/SvcV-8/9. Instead, the documents listed are presently under development and in "working" or "draft" status. The emerging standards will be reviewed on a regular basis to determine whether a status change has occurred.



The emerging standards are also included in the I2R2. The I2R2 acts as both the StdV-1 and the StdV-2 for the DoD IEA v2.0 and enables users to search guidance and policy documents based

on various characteristics of the document. In addition to the standard key word search, R2 provides a status of each document (existing or emerging), categorizes each of the standards to one of seven different document types, as well as the relevant capabilities (CV-2) and services (SvcV-4) in the DoD IEA v2.0. Links to each of the standards contained in the StdV-1 and StdV-2 may also be found in R2. As the DoD IEA continues to evolve and grow, the R2 will be updated with information from the architecture. More information on R2 can be found in Volume 1 of the DoD IEA or at *https://www.intelink.gov/sites/dodieav2/framework/default.aspx*.

The set of standards in this StdV-2 are not aligned to expected availability time periods because in most cases this information was not available. As such information becomes available, the information in this table will be revised to contain expected availability.

Table 8.2-1 Standards Forecast (StdV-2)

Standard Title	Related Capability	Related ITESR Initiative	Standard Type
Data Center & Server Consolidation Reference Architecture (DCSC RA)	Architecture Development and Use	Data Center and Server Consolidation	Architecture
GENMA PBNM Architecture - Deliverable 3	Architecture Development and Use; Automated Configuration Changes	Joint Enterprise Network (JEN)	Architecture
Joint Information Environment Operational Reference Architecture (JIE ORA)	Architecture Development and Use; Information Sharing with Mission Partners; Integrated Network Operations Services; NetOps-Enabled Resources	Enterprise Cross Domain Services; Joint Enterprise Network (JEN)	Architecture
Network Optimization Reference Architecture (NORA)	Architecture Development and Use; Integrated Network Operations Services; NetOps-Enabled Resources	Joint Enterprise Network (JEN)	Architecture
Unified Capabilities Reference Architecture (UC RA)	Architecture Development and Use; Unified Communications and Collaboration	Enterprise Cross Domain Services	Architecture
CJCSI 6211.02D - Defense Information System Network (DISN) Unified Capabilities: Policy and Responsibilities DRAFT	Standard Guidance; Unified Communications and Collaboration	Enterprise Cross Domain Services; Joint Enterprise Network (JEN)	Policy

Standard Title	Related Capability	Related ITESR Initiative	Standard Type
FIPS 140-3 - DRAFT - Security Requirements for Cryptographic Modules	Information Dissemination Management; Infrastructure Certification and Accreditation; Standard Guidance	Identity and Access Management (IdAM)	Policy
Army Staffing of the Army Data Center and Server Consolidation Plan Initial Draft	Oversight of IE Implementation	Data Center and Server Consolidation	Strategy
Input to DoD IT Near Term Implementation Plan - 2011 Jul 1 - Draft v1.1	Oversight of IE Implementation	Data Center and Server Consolidation	Strategy
NIST SP800-144: DRAFT Guidelines on Security and Privacy in Public Cloud Computing	Network Defense; Oversight of IE Implementation	TLA Stacks	Strategy
NIST SP800-146: DRAFT Cloud Computing Synopsis and Recommendations	Oversight of IE Implementation	TLA Stacks	Strategy
NIST SP800-30 Rev. 1 - DRAFT Guide for Conducting Risk Assessments	IE Operations Threat Assessment; Supply Chain Risk Assessment	TLA Stacks	Strategy

9 Linkage of Activities, Services, Rules to Capabilities

9.1 Introduction

This section extends the description of the IE capabilities begun in Section 5.0 of this document by aligning to each IE capability the activities performed to enable that capability, the services required to deliver that capability or key aspects of it, and the rules constraining the performance of those activities and services in achieving the capability. An Excel workbook (click on icon below) showing this alignment is provided separately in a file titled: “IE Capability Description.xlsx”.

IE Capability Descriptions

9.2 Capability to Activity Relationships

The alignment of operational activities to each IE capability provides users of the DoD IEA with an understanding of the activities that need to be performed to enable that capability. The operational activities aligned to each IE capability were taken from the OV-5a Operational Activity Decomposition Tree (sub-section 3.3 and Appendix C). This alignment represents those activities whose performance is necessary, but not necessarily sufficient, for the capability to be achieved. The activities also have different relationships to the capability, depending on the nature of each activity itself. Some activities are performed to acquire services or other resources that achieve the capability. Others are performed directly by services or other resources to achieve the capability. Still others are performed to manage or operate services or other resources within the IE so they can achieve the capability. It is possible for the activities aligned to any particular capability to exhibit any or all of these perspectives. So a careful examination of an activity's definition is required to ensure its relationship to the capability with which it is aligned is properly understood and can be effectively analyzed in determining the proper actions to be taken to achieve the capability. The alignment of activities to IE capabilities is also captured in the CV-6 Capability to Operational Activities Mapping view, provided in a separate Excel workbook located in a file titled: "Capability to Operational Activities Mapping (CV-6).xlsx".

Capability to
Operational Activities

9.3 Capability to Services Relationships

The alignment of services to each IE capability provides users of the DoD IEA with a better understanding of the resources and associated processes needed to achieve each capability. Ideally, each service should represent a collection of DOTMLPF-P elements required to perform the functions necessary to achieve a capability or part of a capability. How the service operates in the IE to achieve the capability or capabilities is constrained by principles and/or rules. Each service has a prescribed interface that is registered in the IE to provide a standard means for locating and using it. The interface description also provides the user with an explanation of the expected result(s) of invoking the service through its interface.

The services aligned to each capability in this version of the DoD IEA were taken from existing service descriptions, many of which are focused on the IT or materiel aspects of achieving the capability. They represent a necessary, but not necessarily sufficient, set of performers for achieving each capability's desired end-state. In this version of the DoD IEA, the service descriptions provide a general, high-level description of what each service can do, rather than what must be done, to achieve the capability. The alignment of services to IE capabilities is also captured in the CV-7 Capability to Services Mapping view, provided separately as an Excel workbook in a file titled: "CV-7 Capability to Services Mapping_Final DoD IEA v2.0.xlsx".

Capability to
Services Mapping (CV

9.4 Principles/Rules Relationship to Capabilities

The alignment of principles and rules to each IE capability provides users of the DoD IEA with a better understanding of constraints that have been imposed on achieving each capability. They represent specific guidelines the DoD CIO is establishing for the IE and its operation. They provide the user with a scope for each capability, describing required aspects of the end-state when the capability is achieved and/or setting specific results for a capability. The principles and rules may also place controls, conditions, and/or standards on how activities are to be performed and services executed in achieving a capability.

The current set of principles and rules aligned with IE capabilities were taken from previous versions of the DoD IEA and operational outcomes for the IE defined by the GIG 2.0 ORA. The principals and rules assigned to each IE capability should be considered necessary, but not necessarily sufficient, to achieve that capability in the context of a DoD CIO-managed IE. In this version of the DoD IEA, the principles and rules have also not been directly aligned with operational activities and services assigned to each capability. Such an alignment requires additional analysis to determine where and how each rule should best be applied to the activities and services aligned with each capability in order to achieve required results. In addition, how each principle and rule would constrain any given activity will depend upon that activity's perspective in regards to the capability, as previously discussed.

10 Way Ahead

The DoD IEA v2.0 describes the vision for the future IE and the initial set of capabilities it must provide to enable DoD Mission Area and Component operations. The DoDI 8210 Enterprise Architecture in the DoD contains language that establishes the DoD IEA as the authoritative architecture for the IE. The DoD IEA v2.0 focuses primarily on warfighter operational requirements that include a smaller set of operational requirements that are common across all Mission Areas and Components. It was also developed using information from existing sources with differing purposes, scopes, and perspectives. The continued evolution of the DoD IEA will enhance the capabilities to address unique mission area and component requirements; refine and better focus the activities, rules, functions, and services used to achieve the IE capabilities; and increase the level of detail and analysis to further support IT investment decision making and solution development for the IE.

10.1 Additional Vetting of Contents with Subject Matter Experts

Vetting current DoD IEA v2.0 information and analysis with relevant subject matter experts (SME) is the first step in continuing the evolution of the DoD IEA. Future versions of the DoD IEA will:

- Provide a complete and more comprehensive set of IE Capability Descriptions − The capabilities in the current taxonomy have only been vetted with a very limited group of SMEs and may not represent the full scope of requirements for the IE. A more robust vetting process, with relevant stakeholder SMEs, is needed. This will result in an enhanced and extended set of IE capabilities with more comprehensive definitions, and a proper level of decomposition for the CV-2 to improve usefulness to all stakeholders. Specifically, the next version of the IEA will:
    - Refine previously incorporated Information Assurance (IA) and other NSA related capabilities
    - Incorporate accepted Spectrum Management capabilities
- Provide a complete and more comprehensive set of activities that are IE capability based− the activities and IE capabilities were assembled from existing sources with differing perspectives and purposes, and they did not necessarily align well. A managed vetting process, with relevant stakeholder SMEs, to identify and define the complete set of activities based on vetted capabilities is needed. This will result in activity decompositions that are more closely aligned to the required capability taxonomy and provide sufficient detail to derive the functions needed to perform the activities. This may also lead to a more effective association of rules to capabilities through the activities. Specifically, the next version of the IEA will:
    - Incorporate accepted Information Assurance (IA) and other NSA related activities
    - Incorporate accepted Spectrum Management activities
    - Refine activity definitions with accepted definitions recommended by the USMC
    - Incorporate accepted Governance activities from the JIE effort
- Identify a comprehensive set of service functions required to deliver a given capability − Existing service descriptions are aligned to the capabilities and this alignment may not adequately describe what is needed to achieve the capability. If a comprehensive set of functions are identified, they can be grouped into required service descriptions that define the full set of DOTMLPF-P elements needed to perform the identified functions. This set of required service descriptions would provide a more objective and comprehensive requirements baseline against which to assess the ability of given initiatives and programs to deliver the service solutions required for effective achievement of each capability.
- Provide performance measures for the capabilities − Available information did not identify or permit alignment of performance measures to the IE capabilities. The identification of a set of performance measures that establishes when the capability has been effectively achieved is needed. Fully vetted capabilities will facilitate SME

identification of the performance measures necessary to determine capability achievement.

- Provide detailed relationships and dependencies among the capabilities − Understanding the relationships and dependencies among the capabilities is necessary to prioritize capabilities in strategic planning and for assessing development and acquisition efforts. Dependencies between capabilities are best determined in the context of an operational scenario. Use of selected Joint Mission Threads (JMTs) as scenarios can provide a means to determine capability interdependencies.
- Provide more comprehensive detail for applying DoD IEA content and complying with the DoD IEA. This will include the introduction of an automated means for showing compliance with the DoD IEA.

10.2 Evolution of IEA Information Reference Resource

A key element in assisting the user of the DoD IEA is to make the information as available, transparent, and organized for rapid use. A set of criteria describes the elements of compliance with the IEA. The I2R2 was developed to enhance the usability of the IEA and will continue to be improved in order to create a tool that is integral to the IEA and of greatest utility to those who need it most (architects and decision-makers).

10.3 Work with Stakeholders of IEA on relationships to DoD CIO Management Activities

In this version of the DoD IEA, Volume I was introduced to start the more effective use of the IEA by the DoD CIO. As such, the uses of the IEA have only been touched on and need further collaboration with stakeholders and decision makers in order to more fully utilize the IEA as a valuable tool. To that goal, future versions of the IEA will address how the IEA can be better integrated into DoD CIO governance activities and help develop and manage policy that will usher in better enterprise-wide capabilities for the Department.

Appendix A: Acronyms and Glossary

Acronyms

AoR	Area of Responsibility
C2	Command and Control
CCMD	Combatant Command
CI	Computing Infrastructure
CIO	Chief Information Officer
CIR	Computing Infrastructure Readiness
COI	Community of Interest
CPM	Capability Portfolio Manager
CR	Communications Readiness
CSP	Computing Service Provider
CT	Cipher Text
DDMS	DoD Discovery Metadata Specification
DECC	Defense Enterprise Computing Center
DoD IEA	Department of Defense Information Enterprise Architecture
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	Department of Defense
DoDD	DoD Directive
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy
DSD	Data and Services Deployment

DSDR	Data and Services Deployment Business Rules
EIE	Enterprise Information Environment
FEA	Federal Enterprise Architecture
GCN	GIG Computing Node
GIG	Global Information Grid
I2R2	IEA Information Reference Resource
IA	Information Assurance
IC	Intelligence Community
IdM&A	Identity Management and Authentication
IE	Information Enterprise
IEA	Information Enterprise Architecture
IM	Information Management
IP	Internet Protocol
IPv6	Internet Protocol version 6
IRB	Investment Review Board
IT	Information Technology
JCIDS	Joint Capabilities Integration and Development System
JFC	Joint Force Commander
NCES	Net-Centric Core Enterprise Services
NCOW RM	Net-Centric Operations and Warfare Reference Model
NGO	Non-Governmental Organization
NOA	NetOps Agility
OHIO	Only Handle Information Once
PEO	Program Executive Officer

PKI	Public Key Infrastructure
PM	Program Manager
SA	Secured Availability
SLA	Service Level Agreement
SM	Spectrum Management
SNMPv3	Simple Network Management Protocol version 3
SOA	Service-Oriented Architecture
TTP	Techniques, Tactics, and Procedures

Glossary

Accessible: Data and services can be accessed via the GIG by users and applications in the enterprise. Data and services are made available to any user of application except where limited by law, policy, security classification, or operational necessity.

Architect: Any individual, group, or organization within DoD responsible for developing and maintaining, governing, and/or supporting the use of architectures.

Architecture: Fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution. [Source: ISO/IEC 15288:2008 (IEEE Std 152882008), Systems and software engineering System life cycle processes. 4.5.; as extended in the DoD Architecture Framework]

Architecture Description: A representation of a defined domain, as of a current or future point in time, in terms of its component parts, how those parts function, the rules and constraints under which those parts function, and how those parts relate to each other and to the environment.

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Authorization: Permission granted by properly constituted authority to perform or execute a lawful governmental function.

Authorized User: Any appropriately cleared individual with a requirement to access a DoD information system in order to perform or assist in a lawful and authorized governmental function.

Availability: Timely, reliable access to data and information services for authorized users.

Bandwidth: The amount of information or data that can be sent over a network connection in a given period of time. It is usually measured in bits per second, kilobits per second, or megabits per second.

Capability Architecture: Architecture description containing decomposition of DoD activities against which all budgets are aligned and capabilities managed as portfolios. The Business Enterprise Architecture (BEA) is an example of a collection of capability architectures covering areas such as Finance, Human Resources, Acquisition, etc.

Capability Vision: The Capability Vision is a view into the potential end-state of the IE highlighting the “implementation” architecture reference model for the IE and the near term visibility in to the technologies that will be used to implement the Capability Vision for the IE.

Common Core: A set of concepts that have broad applicability across two or more Communities of Interest, but are not universal.

Communications Readiness (CR): Ensures that an evolvable transport infrastructure is in place that provides adequate bandwidth and access to GIG capabilities. The transport functions must provide an end-to-end, seamless net-centric communications capability across all GIG assets.

Community of Interest (COI): Collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have a shared vocabulary for the information they exchange.

Component: See DoD Component.

Computer Network Defense (CND): Describes the actions taken, within the Department of Defense (DoD), to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks. CND protection activity employs information assurance principals and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information.

Computing Infrastructure Readiness (CIR): Provides the necessary computing infrastructure and related services to allow the DoD to operate according to net-centric principles. It ensures that adequate processing, storage, and related infrastructure services are in place to dynamically respond to computing needs and to balance loads across the infrastructure.

Confidentiality: Assurance that information is not disclosed to unauthorized entities or processes.

Constraints: Provide practical guidance for implementing activities and complying with rules by serving as controls on activities. Constraints are generally references to strategic documents or DoD Directives; however, there are constraints that are working groups, websites, and other "resources" that control the activity.

Content Management: The functional capabilities and operational processes necessary to monitor, manage, and facilitate the visibility and accessibility of information within and across the GIG.

Core Enterprise Services: Small set of services, whose use is mandated by the CIO, to provide awareness of, access to, and delivery of information on the GIG.

Cyberspace Operations: Military operations conducted within the cyberspace domain whose primary objective is to ensure the availability, control, and superiority of the battlespace. Effective cyberspace operations enable military operations in other warfighting domains.

Data and Services Deployment (DSD): Decouples data and services from the applications and systems that provide them, allowing them to be visible, accessible, understandable and trusted. DSD guides the building and delivery of data and services that meet defined needs but are also

able to adapt to the needs of unanticipated users. DSD lays the foundation for moving the DoD to a Service-Oriented Architecture (SOA).

DoD Information Enterprise: The Department of Defense information resources, assets, and processes required to achieve an information advantage and share information across the Department and with mission partners. It includes: (a) the information itself, and the Department's management over the information lifecycle; (b) the processes, including risk management, associated with managing information to accomplish the DoD mission and functions; (c) activities related to designing, building, populating, acquiring, managing, operating, protecting and defending the information enterprise; and (d) related information resources such as personnel, funds, equipment, and information technology, including national security systems.

Demarcation: Delineation of domain or ownership area; demarcation of the transport infrastructure occurs at the users interface (i.e., Network Interface Card at the rear of the computer, antenna output jack or connection at the rear of the transmitter/receiver). It is not specific to the type of computer or system within a net-centric environment.
Discovery: The process by which users and applications can find data and services on the GIG, such as through catalogs, registries, and other search services.

DoD Component: One of the following offices that compose the Department of Defense according to DoDD 5100.1:

- The Office of the Secretary of Defense
- The Military Departments
- The Office of the Chairman of the Joint Chiefs of Staff
- The Combatant Commands
- The Office of the DoD IG
- The Defense Agencies
- The DoD Field Activities
- Such other offices, agencies, activities, and commands established or designated by law, the President, or the Secretary of Defense.

DoD Enterprise Information Environment (EIE): The Mission Area that provides the enterprise-wide functions and services that enables the execution activities in the other DoD Mission Areas (i.e., business, warfighter, intelligence) [DoDD 8115]. That is, this Mission Area is responsible for the "implementation" of an operating instance of the IE that supports realization of the support to the other Mission Areas and is critical to operation of the IE in the context of the EA. Nominally, the categories of functionality that is provided is the following: Communications/Network/Transport, Computing Infrastructure, Enterprise Services, Information Assurance, Information and Data Management, NetOps, and support to end-user access. As such, this definition subsumes the definition of the GIG.

DoD Information Enterprise: The DoD information resources, assets, and processes required to achieve an information advantage and share information across the Department of Defense and with mission partners. It includes:

a. The information itself and the Department's management over the information lifecycle
b. The processes, including risk management, associated with managing information to accomplish the DoD mission and functions
c. Activities related to designing, building, populating, acquiring, managing, operating, protecting, and defending the information enterprise
d. Related information resources such as personnel, funds, equipment, and IT, including national security systems. (DoDD 8000.01)

The purpose of the DoD Information Enterprise is to support the development, management, and use of information for the benefit of all DoD stakeholders' mission requirements.

DoD Information Enterprise Architecture (IEA) - A description of the integrated defense information enterprise and the rules for the information assets and resources that enable it. The DoD IEA unifies the concepts embedded in DoD net-centric strategies into a common vision, highlighting the key principles, rules, constraints, and best practices drawn from collective policy to which applicable programs must adhere. [Draft DoDI 8210]

The IEA is the architecture for the management of the DoD information enterprise, providing the requirements for its realization. The IEA will contain a description of the relevant viewpoints of the stakeholders of the IE including all components of the DoD Enterprise utilizing the IE to enable net-centric operations for all DoD Missions.

DoD Enterprise Architecture: A federation of descriptions that provide context and rules for accomplishing the mission of the Department. These descriptions are developed and maintained at the Department, Capability Area, and Component levels and collectively define the people, processes, and technology required in the "current" and "target" environments; and the roadmap for transition to the target environment. (DoDD 8000.01)

A collection of artifacts (policy, strategy, and guidance documents; enterprise reference architectures; registered "fit-for-federation" CC/S/A architectures) describing viewpoints of enterprise stakeholders.

End-to-End: An environment in which all activities associated with the flow and transformation of information encompass the source of the information (i.e., the producer) to the recipients (i.e., the consumers, or end-users).

Enterprise Architecture (EA): [PROPOSED] An enterprise architecture (EA) [as a noun] is a rigorous description of the structure of an enterprise, which comprises enterprise components (business entities), the externally visible properties of those components, and the relationships

(e.g. the behavior) between them. EA describes the terminology, the composition of enterprise components, and their relationships with the external environment, and the guiding principles for the requirement (analysis), design, and evolution of an enterprise. This description is comprehensive, including enterprise goals, business process, roles, organizational structures, organizational behaviors, business information, software applications and computer systems. [Source: Wikipedia]

> The EA is the explicit description and documentation of the current and desired relationships among business and management processes and information technology. EA provides the top-down guidance across capabilities and organizations.
>
> Enterprise architecture is also a professional practice committed to the skills necessary to describe an enterprise and assist in translating the strategy for the enterprise into a realization of that strategy through people, process, and technology.

Enterprise Management: The functional capabilities and operational processes necessary to monitor, manage, and control the availability, allocation, and performance within and across the IE. Enterprise Management includes Enterprise Services Management, Applications Management, Computing Infrastructure Management, Network Management, Satellite Communications Management, and Electromagnetic Spectrum Management.

Federated Architecture: An approach for enterprise architecture development that is composed of a set of coherent but distinct entity architectures—the architectures of separate members of the federation. The members of the federation participate to produce an interoperable, effectively integrated enterprise architecture. The federation sets the overarching rules of the federated architecture, defining the policies, practices and legislation to be followed, as well as the interfederate procedures and processes, data interchanges, and interface standards, to be observed by all members. Each federation member conforms to the enterprise view and overarching rules of the federation in developing its architecture. Internal to themselves, each focuses on their separate mission and the architecture that supports that mission.

Federated Enterprise Architecture: An approach for enterprise architecture development that is composed of a set of coherent but distinct entity architectures—the architectures of separate members of the federation. The members of the federation participate to produce interoperable, effectively integrated enterprise architecture. The federation sets the overarching rules of the federated architecture, defining the policies, practices and legislation to be followed, as well as the inter-federate procedures and processes, data interchanges, and interface standards, to be observed by all members. Each federation member conforms to the enterprise view and overarching rules of the federation in developing its architecture. Internal to themselves, each focuses on their separate mission and the architecture that supports that mission. [Draft: DoD CIO Federation Strategy, 2011]

Gap Analysis: An architecture evaluation comparing the current IT environment with requirements established by an architecture to assess how well those requirements can be met with existing capabilities. The resulting IT "gaps," along with corresponding IT "redundancies" and "dead-ends," represent issues for which the decision-maker and/or program manager must provide resolutions to meet net-centric goals and objectives.

Global Information Grid (GIG): The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network. [DoDD 8000.01]

IE Situational Awareness: The ability to acquire and share information across and external to the IE in a manner that enables users, operators, and Commanders to attain timely and accurate, shared understanding of the health and mission readiness of the IE in order to proactively support current, planned and potential future operations.

Information Assurance: Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Information Enterprise (DoD): The DoD information resources, assets, and processes required to achieve an information advantage and share information across the Department of Defense and with mission partners. It includes: (a) the information itself and the Department's management over the information life cycle; (b) the processes, including risk management, associated with managing information to accomplish the DoD mission and functions; (c) activities related to designing, building, populating, acquiring, managing, operating, protecting, and defending the information enterprise; and (d) related information resources such as personnel, funds, equipment, and IT, including national security systems.

Information Enterprise Key Functions: Derived top-level functions (categories of functionality) representing the aggregated activities required of the information enterprise necessary to meet the needs of the stakeholder's (primarily the Warfighters for this instance of the DoD IEA) systems and services as they interact with the rest of the DoD Enterprise. The activities described are those that will define how to accomplish the Capabilities needed by the IE.

Information Management: The discipline that analyzes information as an organizational resource. It covers the definitions, uses, value, and distribution of all data and information within an organization whether processed by computer or not. It evaluates the kinds of data/information an organization requires in order to function and progress effectively.

Infrastructure: A set of interconnected structural elements that provide the framework supporting an entire structure.

Integrity: Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Interoperability: Ability of elements within an information system to communicate with each other and exchange information. Interoperability non-exclusively references data formats, signal levels, physical interface characteristics, logical or relational alignments, and transmission methods or media types.

Inter-organizational Federation: Managed cooperation between nominally co-equal entities (e.g., cooperation between DoD and coalition MoDs, between DoD and DHS, etc.).

Investment Management: Investment management is a process for linking IT investment decisions to an organization's strategic objectives and business plans. Generally, it includes structures (including decision-making bodies known as IRBs), processes for developing information on investments (such as costs and benefits), and practices to inform management decisions (such as investment alignment with an enterprise architecture). The federal approach to IT investment management is based on establishing systematic processes for selecting, controlling, and evaluating investments.

Joint Capability Area (JCA): Collections of similar capabilities logically grouped to support strategic investment decision-making, capability portfolio management, capability delegation, capability analysis (gap, excess, and major trades), and capabilities-based and operational planning. JCAs are intended to provide a common capabilities language for use across many related DOD activities and processes and are an integral part of the evolving capability-based planning (CBP) process.

Joint Future Concept: A visualization of future operations that describes how a commander, using military art and science, might employ capabilities to achieve desired effects and objectives. They explore a wide range of capabilities with a transformational mindset to enhance DoD's ability to assure allies, as well as dissuade, deter, or defeat potential adversaries. Joint future concepts are not limited nor constrained by current or programmed capabilities. They link strategic guidance to the development and employment of future joint force capabilities and serve as "engines for transformation" that may ultimately lead to doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) changes.

Joint Experimentation: The gathering and examining of data related to joint future concepts in order to draw conclusions. Joint experimentation is an iterative process for assessing the effectiveness of varying proposed joint warfighting concepts, capabilities, or conditions as well as evaluating a concept's proposed solutions. The results of joint experimentation can lead to recommendations for the development of new concepts, the revision of existing concepts, or for changes in DOTMLPF-P and policy that are required to achieve significant advances in future joint operational capabilities.

Leaf-Level Activities: The activities that reside at the lowest-level of an activity decomposition.

Manage: Discrete processes that the DoD CIO actively and directly manages.

Management Analysis: An architecture evaluation focusing on use of an architecture description to develop more detailed guidelines for managing investments and programs to meet net-centric goals and objectives and, most importantly, follow net-centric policy. Such an analysis uses the DoD IEA rules, as applied to a supporting architecture, as a starting point for developing more focused rules providing the level of detail needed to actually manage the acquisition of capabilities defined by the architecture. These more detailed rules are extensions, refinements, and/or enhancements of applicable DoD IEA rules. They should be applied by decision-makers and program managers in directing portfolios and programs and as the basis for selecting solutions to meet established needs.

Mechanism: Generally "tools" or resources that provide additional detail on "how" an activity or requirement could be accomplished. Mechanisms are not the only way an activity or requirement could be accomplished, but are rather an example of how it could be accomplished.

Mission Areas (MA): A functional area categorization within the DoD representing major divisions of enterprise business functions (i.e., warfighting, business, defense intelligence, EIE). The Joint Capability Areas (JCAs) provide the capabilities needed to satisfy business of the MAs.

Net-centric Vision: To function as one unified DoD Enterprise, creating an information advantage for our people and mission partners by providing: (1) A rich information sharing environment in which data and services are visible, accessible, understandable, and trusted across the enterprise, and (2) An available and protected network infrastructure (the GIG) that enables responsive information-centric operations using dynamic and interoperable communications and computing capabilities.

NetOps: The Department-wide construct used to operate and defend the GIG to enable information superiority.

NetOps Agility (NOA): Enables the continuous ability to easily access, manipulate, manage and share any information, from any location at any time. NetOps Agility sets policies and priorities necessary to operate and defend the GIG. It establishes common processes and standards that govern operations, management, monitoring and response of the GIG.

NetOps Architecture: A framework or structure that defines the mission, the information and technologies required to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs.

Network Defense: Network Defense describes the functional capabilities and operational processes necessary to protect and defend the GIG to include CND with associated Response Actions and Critical Information Protection.

Non-repudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Oversee: Activities performed by the DoD CIO to monitor and influence the outcomes of DoD CIO-relevant policy decisions, programs, and initiatives.

Priority Areas: The fundamental organizational construct for the DoD IEA. Priority Areas align investments with key net-centric principles. They help transform the enterprise by emphasizing critical needs for achieving the target state of the DoD IE and describing challenges to meeting those needs. The five Priority Areas are: Data and Services Deployment (DSD), Secured Availability (SA), Computing Infrastructure Readiness (CIR), Communications Readiness (CR), and NetOps Agility (NOA).

Reference Architecture: Reference Architecture (RA) is an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions. [Source: Reference Architecture Description, OSD/NII, June 2010]. An RA is essentially realization of one instance of an RM with additional attributes that are inherent to architecture description including: behavior, tailored to a specific purpose, technical guidance, pattern for use, tailoring of terms and vocabulary specific to the architecture's intended use. The DoD IEA is an example of a high-level reference architecture describing the entire information enterprise. RAs, as referenced in the IEA document, are intended to further clarify and standardize how delivered Capabilities, derived from the IEA, will be implemented. Other DoD enterprise-wide RAs are released (e.g., EANCS, ITIORA, Biometrics RA) or under development. Another example of importance to this document is the GIG 2.0 Operational Reference Architecture (ORA) which represents the operational view of the GIG.

Reference Model: A reference model (RM) is a standardized and well recognized (vetted) representation of a domain describing its structure and taxonomy. For example, an "operational" reference model for military decision-making might be the (Observe Orient Decide Act) OODA Loop. A system architecture reference model for computer communication might be the 7-layer OSI model. The Consolidated FEA RM is another example used by the US Federal government for classifying enterprise architecture domains and is made up of a series complementary RMs.

Seamless: Seamless transport of data implies that the user is unaware of the path, speed, capacity or method of transmission for the various datasets used to perform specified tasking or mission elements.

Secured Availability (SA): Ensures data and services are secured and trusted across DoD. Security is provided, but security issues do not hinder access to information. When users discover data and services, they are able to access them based on their authorization. Permissions and authorizations follow users wherever they are on the network. This is a DoD Information Enterprise Architecture priority.

Service: A mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description.

Service Oriented Architecture: An evolution of distributed computing and modular programming. SOAs build applications out of software services. Services are relatively large, intrinsically unassociated units of functionality, which have no calls to each other embedded in them. Instead of services embedding calls to each other in their source code, protocols are defined which describe how one or more services can talk to each other. This architecture then relies on a business process expert to link and sequence services, in a process known as orchestration, to meet a new or existing business system requirement.

Solution Architecture: The fundamental organization of a system, embodied in its components; their relationships with each other and the environment; and the principles governing its design and evolution.

Strategic Architectures: Strategic Architectures are a set of descriptions focused on the rules and principles that apply to all investments regardless of capability/segment, Component or portfolio. The DoD Information Enterprise Architecture (DoD IEA) is a prime example of this type of architecture. It includes rules about how information generated in operations across DoD should be made visible, accessible, and understandable, in a trusted environment for all authorized users, across the Department. Programs must align to this guidance to be funded. Moreover, the DoD IEA contains the information sharing rules applicable to all programs to make information sharing integral to everything the Department does. Because they are so cross-cutting, these types of rules belong in this type of strategic architecture rather than in a modular capability segment. [Source: DoD Enterprise Architecture Strategy (Wiki) - The DoD Architecture Strategy does not represent DoD policy, but rather is a collaborative forum to provide inputs to DoD policy changes in the future.]

Support or Provide: Refers to the DoD IEA-relevant products and services that are paid for, sponsored, or provided by the DoD CIO.

Technical Federation: An enabling concept for net-centric information sharing. Technical federation is a means for achieving interoperability among the diverse and heterogeneous technical components making up the DoD IE. Technical federation makes it possible for these different components to share data and operate together while still preserving their agility and unique characteristics. The federation concept covers areas such as identity management, digital trust, management of name spaces/directory structures, and security enclaves.

Technology Innovation: An enabling concept for net-centric information sharing. Technology innovation involves the specification of target information technologies and associated relationships contributing to the development of net-centric DoD services. Technology innovation involves deriving target technology families from net-centric strategies and other DoD authoritative sources to extend accepted technical standards and describe those technologies which should be adopted to enable net-centric information sharing. Technology

innovation also focuses attention on the need to co-evolve technology and net-centric operational concepts.

Tiered Accountability: Aligns responsibility and accountability for decision making and execution across the tiers of the Department—DoD Enterprise, Component, and Program.

Transport: The collection of interconnected pathways within a network infrastructure that allow information to traverse from system to system or system to user. It is also the movement of information and/or knowledge among consumers, producers, and intermediate entities.

Trusted: Users and applications can determine and assess the suitability of the source because the pedigree, security level, and access control level of each data asset or service is known and available.

Understandable: Users and applications can comprehend the data, both structurally and semantically, and readily determine how the data may be used for their specific needs.

Universal Core: The small set of concepts which are universally understandable and thus can be defined across the enterprise.

Visible: The property of being discoverable. All data assets (intelligence, non-intelligence, raw, and processed) are advertised or "made visible" by providing metadata, which describes the asset.

Appendix B: DoD IEA Principles and Business Rules

The set of principles and rules aligned with IE capabilities in Section 9.4 were taken from previous versions of the DoD IEA and from operational outcomes for the IE defined by the GIG 2.0 ORA. This Appendix provides a complete list of these Principles and Rules as defined and numbered in their original source documents. Future versions of the DoD IEA will re-order and possibly re-number these principles and rules.

DoD IEA Global Principles (GP)

- **GP 01** – Department of Defense (DoD) Chief Information Office (CIO)-governed resources are conceived, designed, operated, and managed to address the mission needs of the Department.
- **GP 02** - Interoperability of solutions across the Department is a strategic goal. All parts of the Global Information Grid (GIG) must work together to achieve this goal. Information is made interoperable by following the rules for net-centric sharing of data and services across the enterprise. The DoD achieves infrastructure interoperability through definition and enforcement of standards and interface profiles and implementation guidance.
- **GP 03** - Data assets, services, and applications on the GIG shall be visible, accessible, understandable, and trusted to authorized (including unanticipated) users.
- **GP 04** - DoD CIO services shall advertise service-level agreements (SLAs) that document their performance, and shall be operated to meet that agreement.
- **GP 05** - The GIG will provide a secure environment for collaborative sharing of information assets (information, services, and policies) with DoD's external partners, including other Federal Departments and Communities of Interest (e.g., Department of Homeland Security, the Intelligence Community), state and local governments, allied, coalition, non-governmental organizations (NGOs), academic, research, and business partners.
- **GP 06** - The DoD Information Enterprise (IE) will include global access to common DoD-wide capabilities and services that enable access to people and information resources from any computer in the world. To the extent possible, services shall be developed for global use. The use of these globally accessible services will improve warfighting effectiveness, and interoperability, while reducing cost.

Data & Services Deployment (DSD)

Data & Services Deployment Principles (DSDP)

- **DSDP 01** - Data, services, and applications belong to the enterprise. Information is a strategic asset that cannot be denied to the people who need it to make decisions.
- **DSDP 02** - Data, services, and applications should be loosely coupled to one another. The interfaces for mission services that an organization provides should be independent of the underlying implementation. Likewise, data has much greater value if it is visible, accessible

and understandable outside of the applications that might handle it.

- **DSDP 03** - Only handle information once (the OHIO principle). Information that exists should be reused rather than recreated.
- **DSDP 04** - Semantics and syntax for data sharing should be defined on a community basis. Information sharing problems exist within communities; the solutions must come from within those communities.
- **DSDP 05** - Data, services, and applications must be visible, accessible, understandable, and trusted by "the unanticipated user". All needs can never be fully anticipated. There will inevitably be unanticipated situations, unanticipated processes, and unanticipated partners. By building capabilities designed to support users outside of the expected set, the Department can achieve a measure of agility as a competitive advantage over our adversaries.

Data & Services Deployment Business Rules (DSDR)

- **DSDR 01** - Authoritative data assets, services, and applications shall be accessible to all authorized users in the Department of Defense, including Joint, interagency, inter-governmental, and multinational partners, and accessible except where limited by law, policy, security classification, or operational necessity.
- **DSDR 02** - All authoritative data producers and capability providers shall describe, advertise, and make their data assets and capabilities available as services on the GIG.
- **DSDR 03** - All authoritative data assets and capabilities shall be advertised in a manner that enables them to be searchable from an enterprise discovery solution.
- **DSDR 04** - Data will be described in accordance with the enterprise standard for discovery metadata (the DoD Discovery Metadata Specification [DDMS]).
- **DSDR 05** - Communities of Interest (COIs) will determine which data sources are authoritative and will not declare any source authoritative without establishing a valid pedigree.
- **DSDR 06** - Mission or business functions will be made available to the enterprise as a network-based service with a published, well-defined interface.
- **DSDR 07** - Services shall be advertised by registering with an enterprise service registry.
- **DSDR 08** - COIs should develop semantic vocabularies, taxonomies, and ontologies.
- **DSDR 09** - Semantic vocabularies shall re-use elements of the DoD Intelligence Community-Universal Core or National Information Exchange Model (NIEM) information exchange schema.
- **DSDR 10** - Vocabularies, taxonomies, and ontologies must be registered with the enterprise for visibility, re-use, and understandability.
- **DSDR 11** - Existing enterprise data, services, and end-user interfaces shall be used whenever possible, practical, and appropriate, instead of re-creating those assets.
- **DSDR 12** - Available Mandatory Core Designated DoD Enterprise Services, as listed in Appendix G, are mandatory for use regardless of capability delivered.

Secured Availability (SA)

Secured Availability Principles (SAP)

- **SAP 01** - The GIG is critical to DoD operations and is a high-value target for many highly motivated and well-equipped adversaries. As such, it must be conscientiously designed, managed, protected, and defended.
- **SAP 02** - The globalization of information technology, particularly the international nature of hardware and software (including supply chain) development and the rise of global providers of Information Technology (IT) and communications services presents a very new and unique security challenge. GIG resources must be designed, managed, protected, and defended to meet this challenge.
- **SAP 03** - Global missions and globally dispersed users require global network reach. Information Assurance mechanisms and processes must be designed, implemented, and operated so as to enable a seamless DoD Information Enterprise.
- **SAP 04** - Agility and precision are the hallmark of 21st century national security operations. Information Assurance mechanisms and processes must be designed, implemented, and operated so as to enable rapid and precise changes in information access and flow, and resource allocation or configuration.

Secured Availability Business Rules (SAR)

- **SAR 01** - DoD information programs, applications, and computer networks shall protect data in transit and at rest according to their confidentiality level, Mission Assurance category, and level of exposure.
- **SAR 02** - GIG infrastructure, applications and services, network resources, enclaves, and boundaries shall be capable of being configured and operated in accordance with applicable policy. Such policy must address differences in enterprise-wide, system high, community of interest, enclave, and operational mission needs.
- **SAR 03** - DoD information services and computer networks shall be monitored in accordance with pertinent GIG-wide SLAs in order to detect, isolate, and react to intrusions, disruption of service, or other incidents that threaten DoD operations.
- **SAR 04** - DoD programs must clearly identify and fund Information Assurance (IA) management and administration roles necessary for secure operation and maintenance of the program. Additionally, provision must be made for adequate training of all users in secure operation.
- **SAR 05** - GIG assets must establish and implement a Mission Assurance capability that addresses hardware, software, and supplier assurance through engineering and vulnerability assessments.
- **SAR 06** - All DoD services that enable the sharing or transfer of information across multiple security levels shall be centrally planned and coordinated, with proposed service enhancements considered first at the enterprise-wide level, then at the regional/organizational level (e.g., DoD Component), then at the service or application level.

- **SAR 07** - All DoD information services and applications must uniquely and persistently digitally identify and authenticate users and devices. These services, applications, and networks shall enforce authorized access to information and other services or devices according to specified access control rules and quality of protection requirements for all individuals, organizations, COIs, automated services, and devices.
- **SAR 08** - Metadata containing access control and quality of protection attributes shall be strongly bound to or associated with information assets and utilized for access decisions.
- **SAR 09** - DoD programs must demonstrate that their network, data assets, services, and applications and device settings that control or enable IA functionality have been established, documented, and validated through a standard security engineering process.
- **SAR 10** - DoD programs should ensure that configuration changes to networks, data assets, services, applications, and device settings can be automatically disseminated and implemented in conformance with GIG-standard configuration processes.

Shared Infrastructure (SI)

Shared Infrastructure Principles (SIP)

- **SIP 01** - GIG infrastructure capabilities must be survivable, resilient, redundant, and reliable to enable continuity of operations and disaster recovery in the presence of attack, failure, accident, and natural or man-made disaster.
- **SIP 02** - The GIG shall enable connectivity to all authorized users.
- **SIP 03** - GIG infrastructure must be scalable, changeable, deployable, and rapidly manageable while anticipating the effects of the unexpected user.

Shared Infrastructure Business Rules (SIR)

- **SIR 01** - GIG infrastructure resources shall be discoverable, and available to both meet the dynamic demand of all mission requirements and support the monitoring and management of the GIG.
- **SIR 02** - GIG infrastructure capabilities shall be designed, acquired, deployed, operated, and managed in a manner which enables continuity of operations and disaster recovery in the presence of attacks, failures, accidents, and natural or man-made disaster to support customer SLAs.

Computing Infrastructure Readiness (CIR)

Computing Infrastructure Readiness Principles (CIRP)

- **CIRP 01** - Computing infrastructure must support all missions of the Department, and provide the edge with effective, on-demand, secure access to shared spaces and information assets across functional, security, national, and interagency domains.
- **CIRP 02** - Consolidation of computing infrastructure fixed-node operations is a desired result for cost efficiencies. It shall not be accomplished, however, at the expense of degrading mission capabilities and operational effectiveness.

- **CIRP 03** - Computing infrastructure must be able to provide secure, dynamic, computing platform-agnostic and location-independent data storage.
- **CIRP 04** - Computing infrastructure hosting environments must evolve and adapt to meet the emerging needs of applications and the demands of rapidly increasing services.

Computing Infrastructure Readiness Business Rules (CIRR)

- **CIRR 01** - Computing infrastructure shall be consolidated, to the greatest extent possible, so that fixed global/regional and deployed virtual CI resources are used efficiently.
- **CIRR 02** - Computing infrastructure shall be computing platform agnostic and location independent in providing transparent real-time provisioning and allocation of shared resources.
- **CIRR 03** - Computing infrastructure shall be responsive to and supportive of the capability needs and requirements of the edge environment, despite intermittent connectivity or limited bandwidth.
- **CIRR 04** - Physical implementation of computing infrastructure shall include transparent interfaces to users to minimize, if not eliminate, degradation in performance and Quality of Service.
- **CIRR 05** - Computing infrastructure capabilities must be robust and agile to respond to increased computing demand, data storage, and shared space requirements.
- **CIRR 06** - Shared computing and data storage resources shall be capable of being discoverable and accessible for virtual management and control across the GIG.
- **CIRR 07** - All GIG computing infrastructure facilities must be accredited, certified, and approved by DoD designated authorities.

Communications Readiness (CR)

Communications Readiness Principles (CRP)

- **CRP 01** - The GIG communications infrastructure shall support full Internet Protocol (IP) convergence of traffic (voice, video, and data) on a single network.

Communications Readiness Business Rules (CRR)

- **CRR 01** - Implement a modular, layered design based on internet protocol for the transport infrastructure.
- **CRR 02** - GIG communications systems shall provide network connectivity to end points (such as Wide and Local Area Networks and direct connections to mobile end-users) in the same or different autonomous systems.
- **CRR 03** - GIG communications systems shall be acquired to support migration to a Cipher Text (CT) core. CT networks and segments shall transport both classified and unclassified encrypted traffic.
- **CRR 04** - GIG communications systems shall provide the flexibility to support network connectivity to all GIG nodes and users, including those changing their points of attachment

among alternate operational and network domains and/or communities of interest.

- **CRR 05** - GIG communications systems shall be designed and configured to be robust, adaptive, and reliable by employing network and configuration management, diverse path cable routing, and automatic rerouting features, as applicable.
- **CRR 06** - Spectrum Management shall incorporate flexible, dynamic, non-interfering spectrum use.

NetOps Agility (NOA)

NetOps Agility Principles (NOAP)

- **NOAP 01** - DoD shall operate and defend the GIG as a unified, agile, end-to-end information resource.
- **NOAP 02** - Share NetOps information with the enterprise by making NetOps data, services, and applications visible and accessible and enable NetOps data to be understandable and trusted to authorized users.

NetOps Agility Business Rules (NOAR)

- **NOAR 01** - The DoD must continue to transform the Network Operations (NetOps) Command and Control (C2) into a unified and agile construct with centralized direction and decentralized execution to effectively respond to unanticipated situations on the time scale of cyber attack.
- **NOAR 02** - The DoD must ensure NetOps functions of Enterprise Management, Content Management, and Network Defense are fully integrated within and across all management domains.
- **NOAR 03** - The DoD must conduct GIG NetOps functions at all operational levels (strategic, operational, and tactical).
- **NOAR 04** - GIG programs must address relevant capabilities for achieving NetOps Agility in Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities.
- **NOAR 05** - Applicable GIG programs must ensure products and services provide the capability to allow a high degree of automation for NetOps C2, and must support dynamic adjustment of configuration and resource allocation.
- **NOAR 06** - GIG resources to include computing infrastructure, communications systems, IA, and services must be NetOps-enabled to provide operational states, performance, availability, and security data/information enabling enterprise-wide situational awareness and performance management to GIG-wide SLAs.
- **NOAR 07** - NetOps metrics shall be developed to measure the health and readiness of DoD data assets, services, and applications in support of the Department’s missions.

GIG 2.0 ORA-Derived Operational Rules (OPR)

Global Authentication, Access Control, and Directory Services Rules

- **OPR 01** – All authorized entities will have one identity and universal credentials that are recognized by all producers of information and services.
- **OPR 02** – All authorized entities will have timely access to critical data, services, and applications from anywhere in the IE.
- **OPR 03** – Enterprise-level directory services will preserve cross domain security while satisfying information transfer requirements.
- **OPR 04** – A comprehensive security policy will be developed that addresses all aspects of Identity Management and Authentication (IdM&A) and provides for realistic opportunities to enforce the greater IA policy requirements.
- **OPR 05** – Design and implement a single authentication mechanism that is usable across the IE regardless of Service affiliation, role, and/or deployment status.
- **OPR 06** – Implement a digital attribute based approach for granting access to information integrated with an overall IA policy and single authentication mechanism approach.

Information and Services "From the Edge" Rules

- **OPR 07** – Tactical edge users are the initial focus for requirements of any operational support activity or program development.
- **OPR 08** – Data is tagged to support rapid smart-push to the edge user based on location, community of interest, and mission.
- **OPR 09** – Edge users have direct information sharing capabilities with peers in and outside their immediate organization, with central processing for their mission, and with strategic assets per their mission requirements.
- **OPR 10** – Provide for the availability of IT capabilities throughout the IE to any authorized user and are easily discoverable through queries and proactive smart-push services.
- **OPR 11** – Develop an information infrastructure based on common standards to support collaboration and information sharing.
- **OPR 12** – Develop end-user services that can be tailored to warfighter needs for specific missions and locations.
- **OPR 13** – Provide roaming profiles optimized to warfighter environment which allows access to their information and services (e.g. data files, personal files, calendar, contact list, email, etc).
- **OPR 14** – All IT services and information stores will be implemented as visible, accessible, understandable, and trusted to authorized (including unanticipated) users.

Joint Infrastructure Rules

- **OPR 15** – Consolidate infrastructure to enable seamless information sharing and increased

speed of action.

- **OPR 16 –** Shift away from the service-centric network construct to an operationally focused construct.
- **OPR 17** – Provide a self managed computing infrastructure limiting the need for human intervention and enabling the optimization of computing infrastructure resources.
- **OPR 18** – Provide a single, secure, and consolidated network domain.
- **OPR 19** – Develop an overarching infrastructure acquisition strategy (hardware, software, etc) and enforce common computing infrastructure standards.
- **OPR 20** – Provide standard extensions, or common gateways, for integration between network domains to enable internal and external collaboration.
- **OPR 21** – Establish Combatant Command (CCMD)-aligned network service centers to shift from Service-centric network construct to an operational (i.e., regional) construct.

Common Policies and Standards Rules

- **OPR 22** – Develop effective enterprise guidance that mandates the fielding and management of common, joint infrastructure.
- **OPR 23** – Develop enterprise acquisition and certification to ensure IE components are purchased and acquired so they are interoperable and universally certified.
- **OPR 24** – Develop common standards and policies that serve as enforcement mechanisms to ensure interoperability.
- **OPR 25** – Develop policies and strategies for providing a joint training approach, the acquisition of IE capabilities, and the evolution of the IE.
- **OPR 26** – Develop a common set of functional policies so that all components of each IE program or system are developed, tested, certified, and deployed with an emphasis on end-to-end enterprise commonality.
- **OPR 27** – Analyze DoD Certification and Accreditation (C&A) policy to address current challenges resulting from multiple Designated Approving Authorities (DAA).
- **OPR 28** – Provide and enforce common standards that are utilized across all services to enable any user at the edge to access the data he/she needs from interoperable systems and services.

Unity of Command Rules

- **OPR 29** – Provide system and network availability, information protection, and information delivery providing the right information to the edge.
- **OPR 30** – Provide effective command and control of the IE through situational awareness of a seamless information environment.
- **OPR 31** – Develop a more agile and integrated force by means of a unified training approach.

- **OPR 32** – Develop, distribute, and assess common guidance regarding CyberCom and Joint Force Commander (JFC) intent for the operation of the IE in a given Area of Responsibility (AoR) to achieve overall unity of effort.
- **OPR 33** – Provide CyberCom with full situational awareness of the IE through common processes, standards and instrumentation, enabling near real-time manipulation of any asset in order to optimize net-centric services.
- **OPR 34** – Realign the necessary C2 relationships to provide joint C2 of the network, including the electromagnetic spectrum, within the battlespace, thus, allowing the commander to focus on the principle warfighting task.
- **OPR 35** – Assign the command of the network within a given theater to the JFC to mitigate operational risk.
- **OPR 36** – Allow the commander to adopt common policies and standards through a common training regimen.

Appendix C: IEA Operational Activity Decomposition Tree (OV-5a)

This appendix contains a more detailed version of the OV-5a view for this architecture than could be provided in the Information Enterprise Architecture (IEA) summary report or even in the separate, more detailed IEA Operational Viewpoint description. The OV-5a diagrams contained in this appendix, however, are still only extracts from the complete activity decomposition done for the IEA. The complete OV-5a for the IEA will eventually be provided on-line as both an interactive html extract from the IBM Rational System Architect tool and in the form of a series of static PowerPoint slides containing the various parent and child diagrams making up the whole activity hierarchy. The complete set of definitions for all activities in the model are contained in the AV-2 (Integrated Dictionary) in Appendix J.

The OV-5a diagrams in this appendix show activities only down to the third level of decomposition; the more detailed activity decomposition found in the complete OV-5a shows activities to the fifth, and in some cases sixth, level of decomposition. The intent is to provide users with enough information to understand the scope and context of the activities required to manage, develop, secure, operate, and use the Information Enterprise (IE). The diagrams in this appendix are also intended to serve as a tool for use in navigating the complete (and much more complex) activity decomposition to locate the leaf-level activities they are interested in and which they must incorporate into their architectures and align and/or conform to meeting compliance requirements. Users can narrow and improve their searches through the complete activity decomposition by first locating in the diagrams here the areas where those leaf-level activities of interest are likely to reside.

The IEA OV-5a was developed by merging activities from the previously published GIG 2.0 Operational Reference Architecture (ORA), v1.5 (March 2011), and the DoD IEA, v1.2 (May 2010). Activities contained in these two existing documents were aligned, normalized, and then combined to form the activity hierarchy discussed here. **Figure C-1** shows the five primary activities necessary to provide a viable IE that can enable warfighter, business, and intelligence net-centric operations while meeting the visionary requirements of the DoD Chief Information Office (CIO) to provide an innovative, unified capability for information sharing across the Department and with mission partners. These primary activities are:

- **Manage and Oversee the IE** – Governs the development and implementation of the IE. Establishes and uses those structures and processes required to provide effective, high-level management and oversight of the components of the IE and its operations. Develops and enforces the required vision, strategy, and guidance to direct the IE so it meets requirements and applicable law, regulation, and policy (LRP), while at the same time delivering the capabilities necessary to fully enable net-centric warfighting, business, and defense intelligence operations for successful mission accomplishment.

- **Protect and Secure the IE** – Develops and implements processes and mechanisms required to guard critical data, capabilities, the Information Technology (IT) infrastructure, and data exchanges within the IE, while providing authentication and non-repudiation of information and transactions to enable assurance and trust. Provides the ability to control user access to data and services, determine vulnerabilities, and prevent the exploitation of these vulnerabilities by both external and internal threats. Enables the monitoring of IE activity, recognition and assessment of security-related incidents, and selection and execution of appropriate responses.

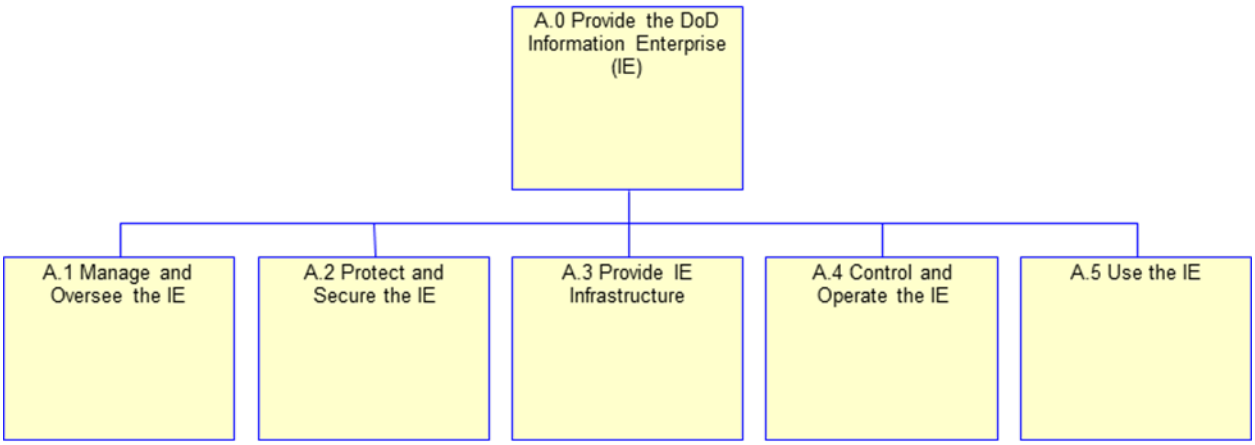


Figure C-1 – Primary IEA Operational Activities

- **Provide IE Infrastructure** – Supplies the enterprise-level communications and computing capabilities required to enable net-centric operations and the enterprise-wide services required by all users. Provides basic IT elements/components which are foundational to the DoD IE and which enable it to fully support assured information sharing across the enterprise and with mission partners.

- **Control and Operate the IE** – Implements capabilities required to provide integrated Network Operation (NetOps) in order to enable information access by any user across network and security domains. Includes processes and mechanisms for Enterprise Management, Content Management, and Network Defense. Enables NetOps to monitor the status and health and direct the actions of DoD IE resources in support of successful accomplishment of joint warfighting, business, and defense intelligence missions.

- **Use the IE** – Enables an authorized user to access the IE and use its functionality to easily discover information, services, and applications, regardless of location, and to assess and critique information, services, and applications based on specific needs in order to improve IE capabilities and service. In support of operations, also enables the user to collaborate and share information with others.

Figures C-2 through **C-6** show activity decompositions to the third level for each of these primary activities. In these separate diagrams, an asterisk (*) has been placed in any activity box for which additional activity decomposition diagrams exist in the complete OV-5a.

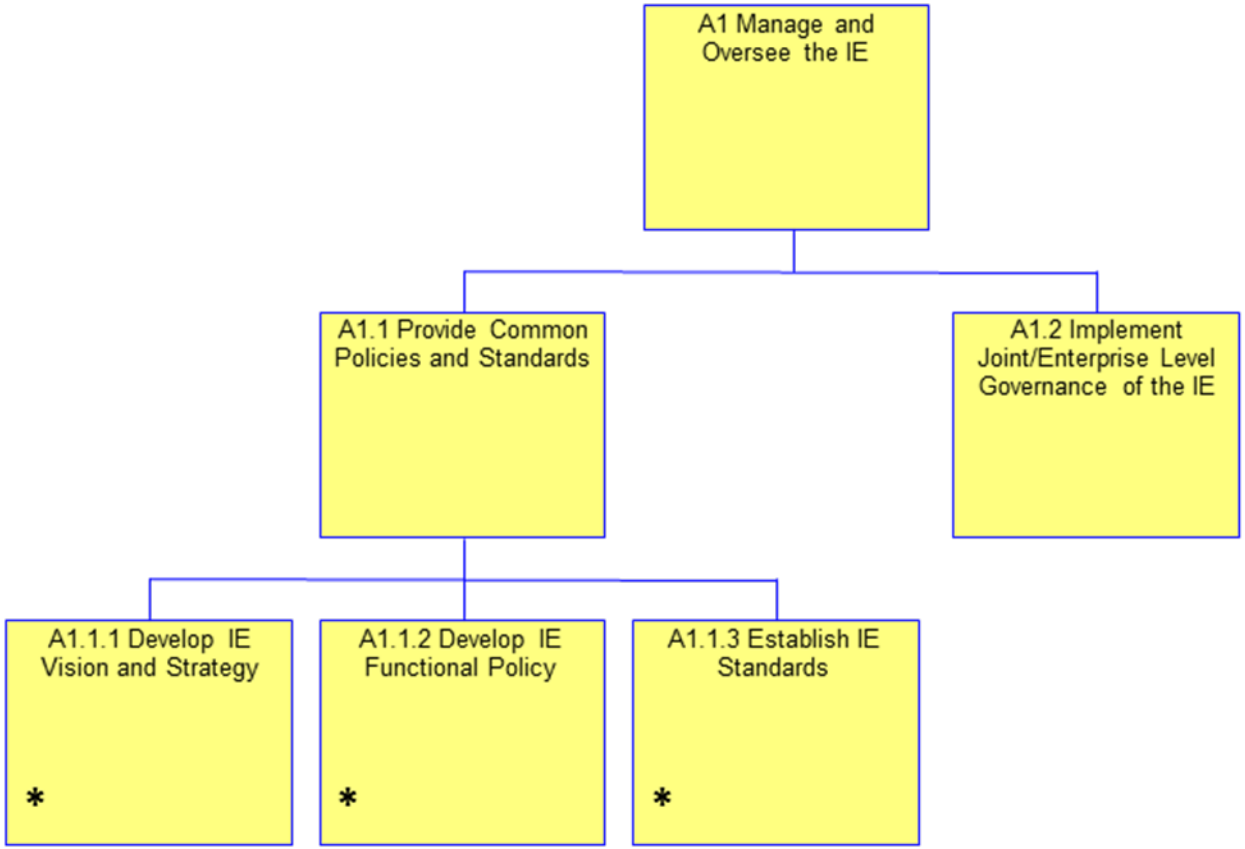


Figure C-2 - Activity Decomposition for Manage and Oversee IE

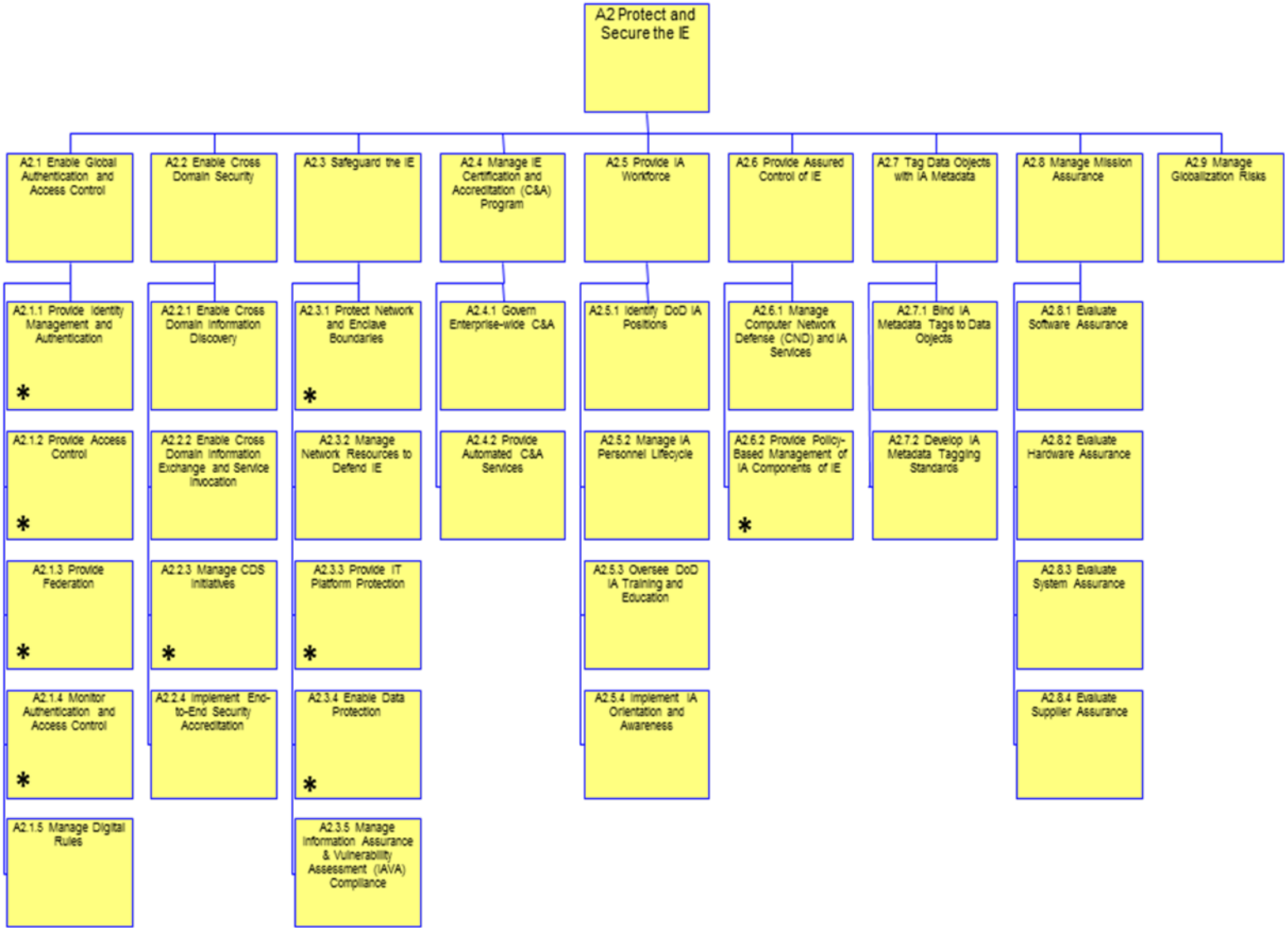


Figure C-3 Activity Decomposition for Protect and Secure the IE

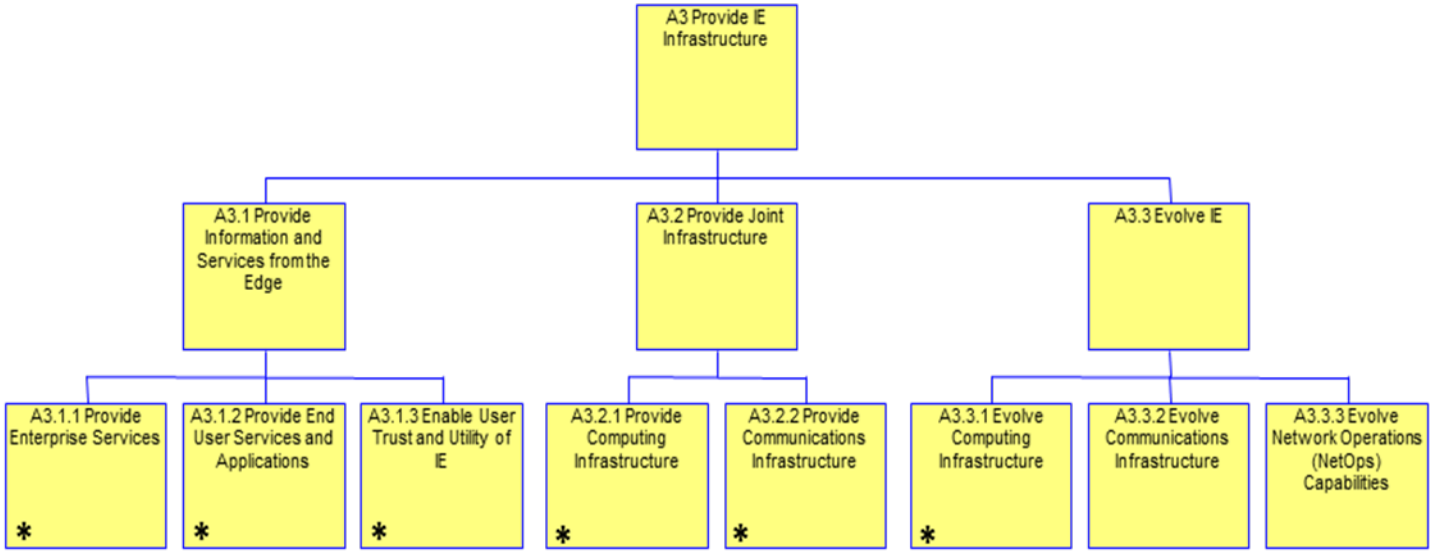


Figure C-4 - Activity Decomposition for Provide IE Infrastructure

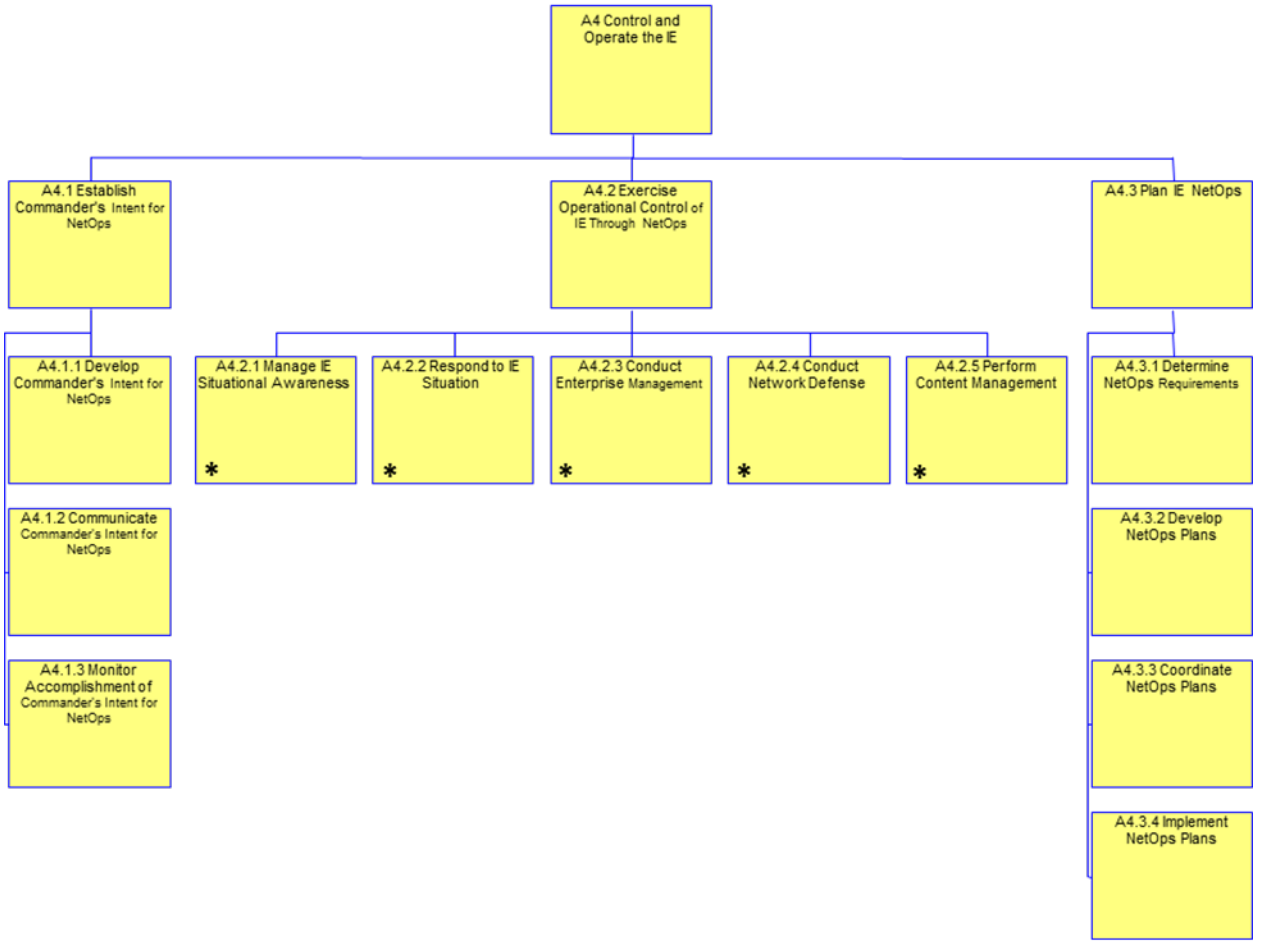


Figure C-5 - Activity Decomposition for Control and Operate the IE

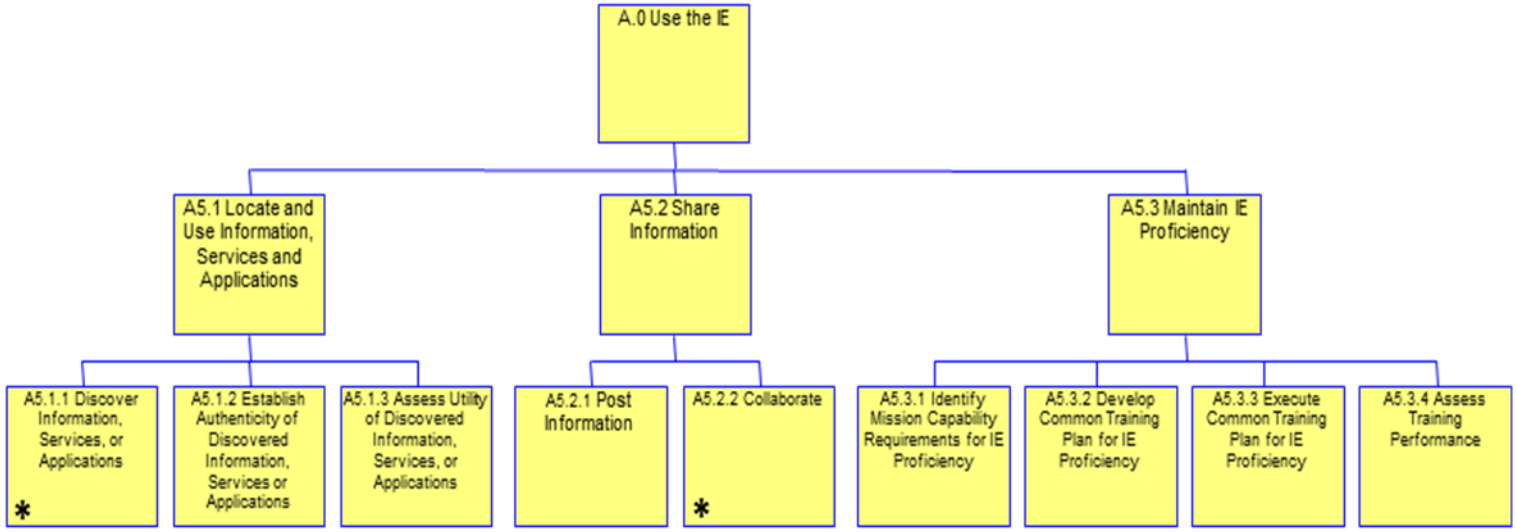


Figure C-6 - Activity Decomposition for Use the IE

Appendix D: Applying the DoD Information Enterprise Architecture (DoD IEA)

1 Purpose

This appendix describes a recommended approach for developing Department of Defense (DoD) architectures so they align with the DoD Information Enterprise Architecture (DoD IEA). It then provides additional detail on how architectures aligned in this way could be used to support/enable the functions of Information Technology (IT) investment managers – to include Portfolio Managers (PfMs) and Investment Review Boards (IRBs) – and managers of IT programs – to include DoD and Component Program Executive Officers (PEOs), Program Managers (PMs), and corresponding functional requirements managers.

2 Relationship of DoD IEA to Other Architectures in the DoD Enterprise Architecture (EA) Federation

A short explanation of how the DoD IEA fits into the DoD Enterprise Architecture (EA) federation provides a better understanding of DoD IEA alignment requirements for different architecture types. **Figure D-1** shows how the DoD IEA fits in the DoD EA federation.

The description of the Information Enterprise (IE) and its requirements – provided by the DoD IEA in the form of IE capabilities and associated activities, rules, and services – is derived from and driven by operational requirements for the IE. Enterprise architectures developed for the business, warfighting, and defense intelligence Mission Areas (MA) are the primary sources of such operational requirements. The DoD IEA may also be influenced to a lesser extent by supplemental, Component-unique operational requirements from Component EAs. By linking the DoD IEA to requirements from the MA and Component EAs it is possible to conduct mission impact and risk analyses to enable trade-off and other investment-related decisions in regards to the IE.

The MA and Component EAs also provide necessary operational context for the DoD IEA. This context supports an understanding of how the IE capabilities should relate to one another in enabling operations. Understanding these relationships allows prioritization of IE capabilities for making investment decisions regarding the use of limited resources to implement solutions delivering desired capabilities. Operational context also supports a determination of how the DoD IEA description should be applied to any given solution architecture and what elements of the DoD IEA should serve as constraints when eventually implementing programs and initiatives governed by these solution architectures.

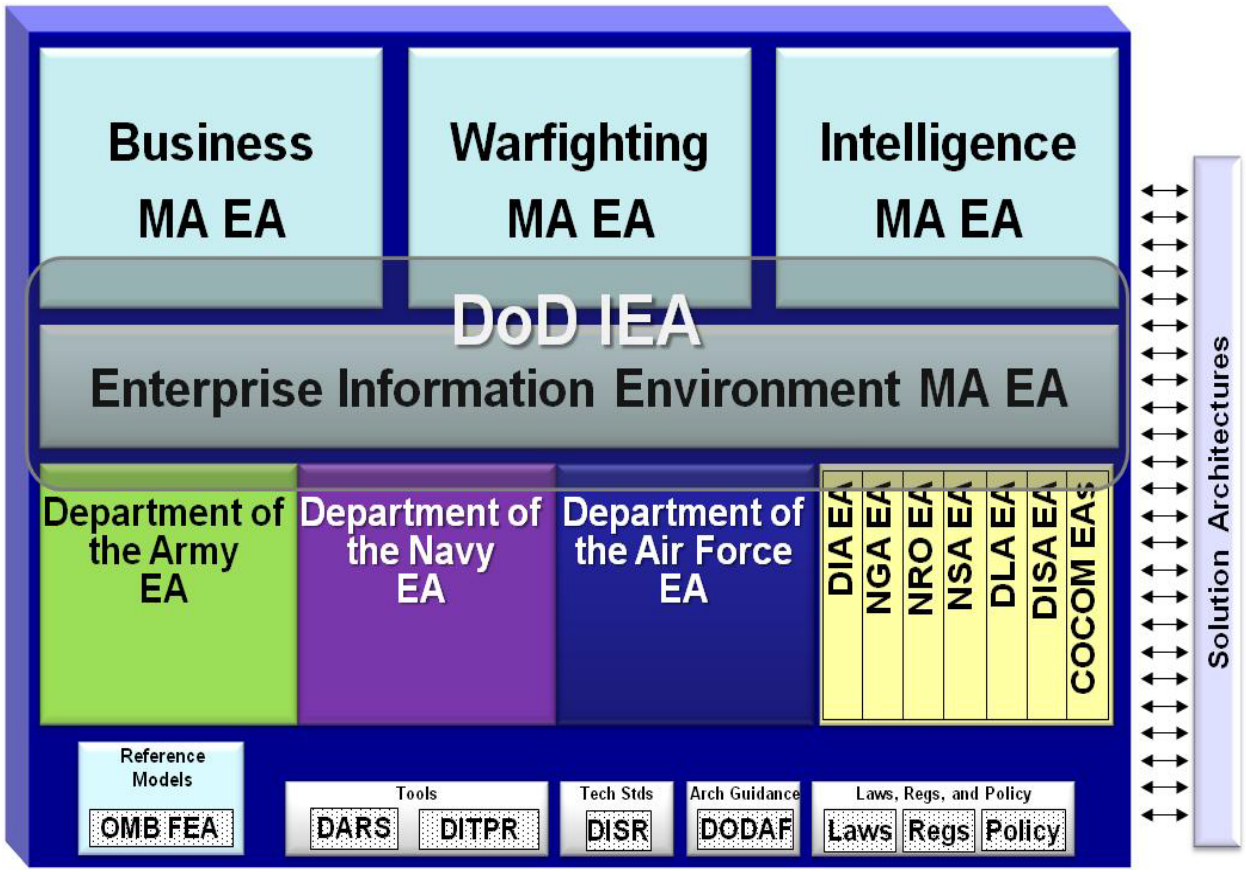


Figure D-1 - DoD Enterprise Architecture (EA)

Most importantly, the Mission Area EAs, Component EAs, and resulting solution architectures are expected to apply the DoD IEA content to guide and constrain interactions within the IE. The DoD IEA is the authorized representation of the desired IE end-state and provides the approved requirements for IT solutions operating in the IE. For this reason, other architectures are expected to comply with the DoD IEA, adopting, expanding upon, and adding detail to these requirements as necessary, but staying within bounds established by the DoD IEA.

In particular, MA EAs will determine touch points where they interact or interface with the DoD IEA, and then point solution architects to the proper elements of the IEA as the source of constraints and/or requirements for those solutions engaging the IE at those points. The Component EAs, on the other hand, will go further, actually incorporating key elements of the DoD IEA (IE capabilities and their associated activities, rules, and services), as applicable, into their architecture descriptions, tailoring those elements to address the unique aspects of the operating environment represented by each Component EA. Solution architectures in turn are required to align with these tailored views of the DoD IEA as presented in each Component EA. How well these other types of architecture align with the DoD IEA will determine how well they guide, direct, or govern the development, acquisition, and implementation of IT solutions able to effectively operate in the IE. In the absence of higher-level, governing architecture that complies

with the DoD IEA, lower-level architecture should comply directly with the DoD IEA. Evidence of this may result in a mapping to the DoD IEA without adopting its vocabulary.

DoD-wide, also called enterprise-level, Reference Architectures (RAs) are also aligned with, and when approved become part of, the DoD IEA, as shown in **Figure D-2**. DoD-wide RAs, as described in the Reference Architecture Description[12], provide "common information, guidance, and direction to guide and constrain architecture and solutions." DoD-wide RAs describe strategic positions, principles and rules, patterns, technical positions, and vocabulary representing the DoD Chief Information Officers' (CIO) direction for achieving common and interoperable solutions across the IE. For this reason, architects are required to conform to these RAs where applicable when developing architectures for IE-related solutions.

3 Architecture Alignment with the DoD IEA

Figure D-2 illustrates the concept behind aligning a DoD architecture that must address the IE with the DoD IEA and then using the resulting aligned architecture to enable IT investment or program management processes. The blocks within the rounded rectangle representing a DoD Architecture are those basic data elements from the DoD Architecture Framework (DoDAF) Meta Model (DM2) that a majority of architectures within DoD are expected to contain. Not all DoD architectures will include all of these data elements, and some may contain additional data elements; however, where these elements do exist in a DoD architecture, they should be aligned wherever necessary and appropriate with the DoD IEA as described here.

As can be seen from this diagram, the alignment of DoD architectures extends beyond simple federation with or incorporation of architectural elements and their descriptions from the main body of the DoD IEA. It also requires alignment with the detailed architecture descriptions of specific IEA functional or capability subsets provided by pertinent, approved DoD-wide RAs. Application of a properly aligned DoD architecture to IT Investment and Program Management will be covered in subsequent sections of this appendix.

3.1 General Architecture Alignment with the DoD IEA

The amount and type of DoD IEA content necessary for effective alignment may vary depending on the type of architecture being developed. Proper alignment for individual architectures is dependent upon the purpose, scope, and questions the architecture is answering. However, the following basic alignment requirements will remain fairly static across architecture types:

[12] The current version of the Reference Architecture Description, dated June 2010, is available from the DoD CIO public web site (http://dodcio.defense.gov/Portals/0/Documents/DIEA/Ref_Archi_Description_Final_v1_18Jun10.pdf). The Reference Architecture Description promulgation memorandum states "the Reference Architecture Description is a detailed overview of the DoD CIO's position on what, generically, constitutes a reference architecture." The memo also says "The Description will be used by the ASRG [Architecture and Standards Review Group] as a metric for compliance when assessing Enterprise-level Reference Architectures."

- Guidance that scopes and bounds the architecture should be aligned with the DoD IEA operational context so the architecture properly addresses warfighter, business, and defense intelligence needs for the IE; this also links IT investments and acquisitions to explicit operational gaps or mission needs and supports analysis of the mission impact of programs and initiatives resulting from the architecture. Architecture guidance should also be aligned with the vision describing the desired technical end-state of the IE so the architecture can guide development and implementation of solutions able to effectively operate in such an IE. This guidance should include an operational concept incorporating a description of how the architecture interacts with the IE, based again on the operational context and IE vision in the IEA.

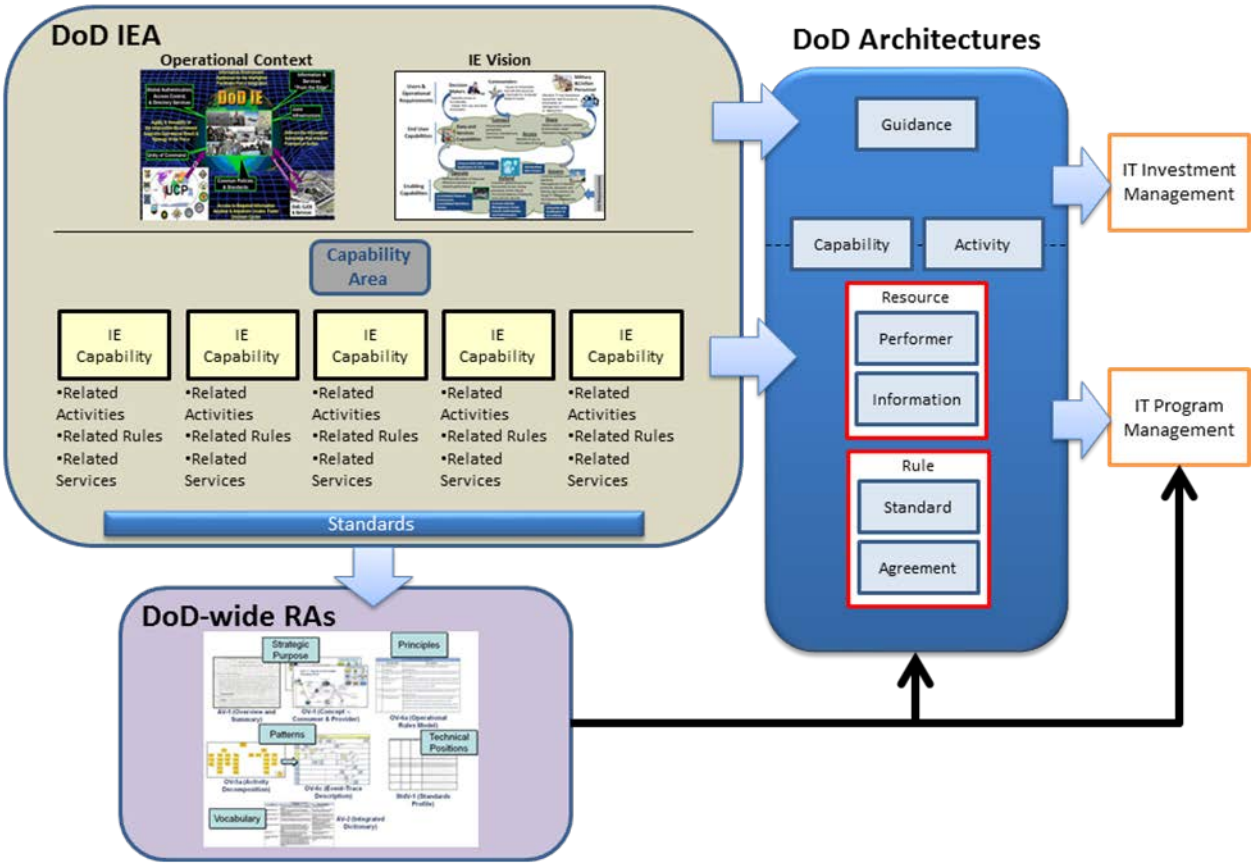


Figure D-2 - Concept for Alignment of DoD Architectures with DoD IEA

- Capabilities described in the architecture should be aligned with pertinent IE capabilities described in the IEA. In cases where the architecture provides one or more IE capabilities, corresponding capability descriptions in the IEA should provide the starting point for more detailed capability descriptions in the architecture. Where IE capabilities from the IEA enable the architecture, the IEA descriptions of these capabilities should guide and constrain the corresponding capability descriptions in the architecture, providing information on where

and how the IE capabilities will interact with the architecture and what they can be expected to provide in support.

- The following elements that make up the more detailed description of each of the IE capabilities in the IEA provide additional information and architecture description that should be applied as appropriate to a DoD architecture:
    - Activities from the DoD IEA should be incorporated into the architecture or serve as starting points for further activity decomposition wherever the architecture needs to describe actions performed to achieve pertinent IE capabilities. They should also be incorporated into the architecture as necessary to constrain how actions or processes that need to occur in the IE are to be performed. Activities from the DoD IEA may also be used in the architecture to describe actions the IE will perform to enable or support the architecture and its interaction with the IE.
    - Services defined in the DoD IEA should provide the basis for descriptions of performers (services, systems, etc.) the architecture will provide to achieve IE capabilities. They also provide information for incorporation into the architecture to describe how IE services enable the architecture and how the architecture should interact with these enabling services.
    - Rules and standards in the DoD IEA should be used to identify, select, and describe more detailed technical rules and specific technical standards for incorporation into the architecture so it can properly constrain the implementation and functioning of solutions in ensuring effective operations in the IE.
- For the most part, IT Investment Management will use the high-level descriptions of operational context, IE vision, and IE capability and associated activities included in capability architectures and Component EAs or pointed to by MA EAs to enable investment decision-making and portfolio construction. On the other hand, Program Management requires the more detailed architecture descriptions of IE capabilities, activities, services, and rules incorporated into Component EAs, DoD-wide RAs, and solution architectures to enable the management of programs and initiatives through their lifecycles.

3.2 Alignment of DoD-wide RAs to DoD IEA

A DoD-wide RA is an extension of the IEA that is scoped around some particular IEA functional or capability subset, adding depth to the IEA architectural description within that functional or capability subset. The RA becomes part of the IEA while also maintaining its identity as a stand-alone architecture. This is notionally shown in **Figure D-3** where a hierarchal taxonomy (capability, service, or activity) of RA A and one of RA B are aligned to the appropriate nodes of one of the corresponding core taxonomies in the DoD IEA. An example of how to use the DoD

IEA in developing a DoD-wide RA is provided in the Use Case: Identify and Develop Reference Architecture Description is found in Appendix I.

For existing RAs the process of aligning to the DoD IEA requires analyses of RA capability, service, and activity views with the corresponding core DoD IEA views to identify the integration points among parent and child nodes. In general, the alignment between a core DoD IEA node and an RA node can be characterized in one of the following ways:

- The RA node is the same as (fully aligns to) a core IEA node
- The RA node is similar to (partially aligns to) one or more core IEA nodes
- The RA node is a child node of one or more core IEA nodes

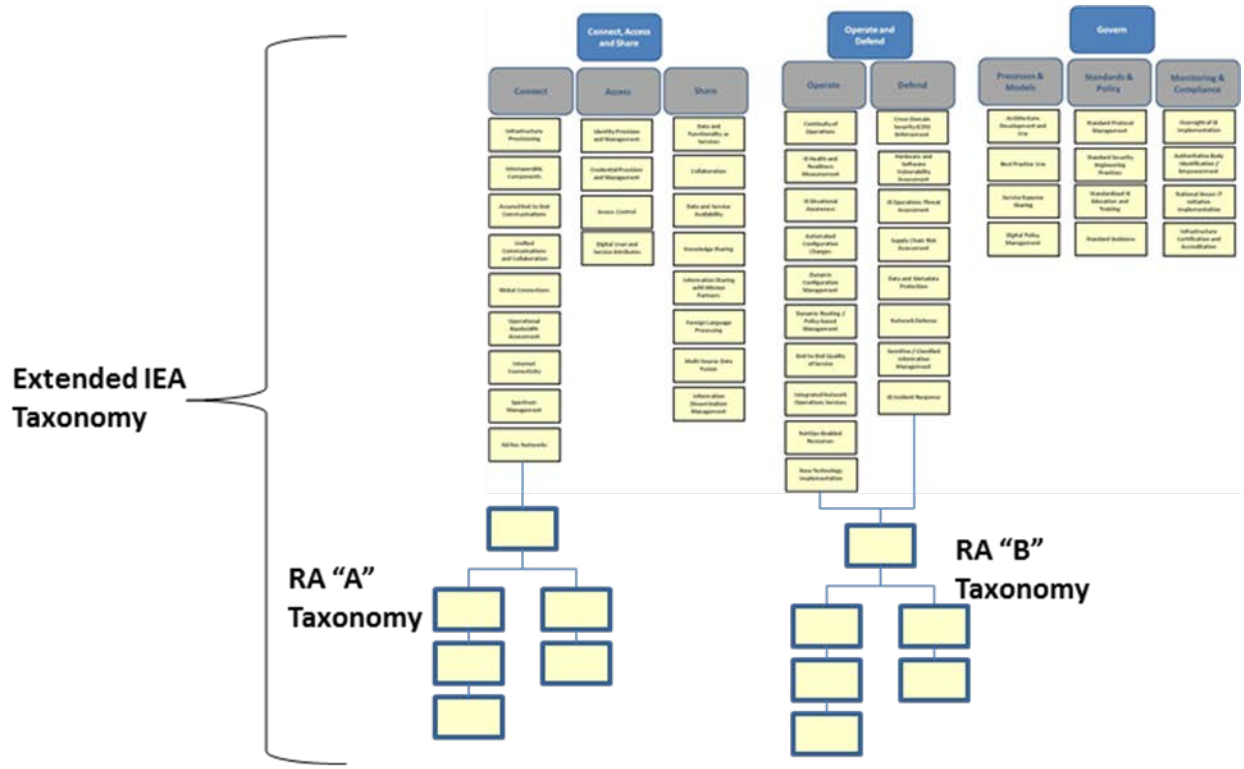


Figure D-3 - Relationship of DoD-Wide RAs to DoD IEA

This type of alignment is similar to processes used within DoD for federating architectures. In a similar fashion, other RA views that are developed (e.g., Rules Models, Standards Models, System views) likewise extend and add detail to the corresponding core IEA views. How existing DoD-wide RAs align to this version of the DoD IEA is shown in the embedded table that follows.

RA Alignment with IE Capabilities.xlsx

For RAs developed subsequent to the publication of this version of the DoD IEA, the alignment between the RA and the DoD IEA will be explicitly established at the outset as part of the RA development process. This will help to ensure that the RA does not overlap other RAs and that the most pressing capability or functional gaps within the IE are prioritized for RA development.

Alignment of DoD-wide RAs with the DoD IEA is achieved by developing the elements of the RA from relevant architecture descriptions in the DoD IEA. A DoD-wide RA builds upon these descriptions, adding additional detail needed to ensure commonality and standardization of solutions built in accordance with the RA. A DoD-wide RA aligns with the DoD IEA in the following ways:

- Derives its strategic positions from the operational context and IE vision provided in the DoD IEA
- Uses capability and associated activity and service descriptions from the DoD IEA in developing patterns
- Derives technical positions from relevant standards identified in the DoD IEA
- Uses rules aligned with relevant capabilities in the DoD IEA in developing principles and rules
- Aligns its vocabulary with the DoD IEA integrated dictionary (AV-2)

As applicable, DoD architectures incorporate or align with the more detailed RA descriptions, and program planning, management, and execution uses appropriate RAs to provide standard solutions. DoD-wide RAs are just one element of a continuum of IE information ranging from enterprise-level policy and strategy to individual programs or initiatives that deliver or manage IE solutions. This is shown in **Figure D-4** which makes it clear that RAs are not typically implemented as a solution per se, but instead feed lower-level and more granular architectures, technical guidance, and programs. The RA developer must consider the role of the RA in this continuum to help ensure that the RA will in fact properly inform and guide the ultimate goal of enabling a particular set of IE capabilities.

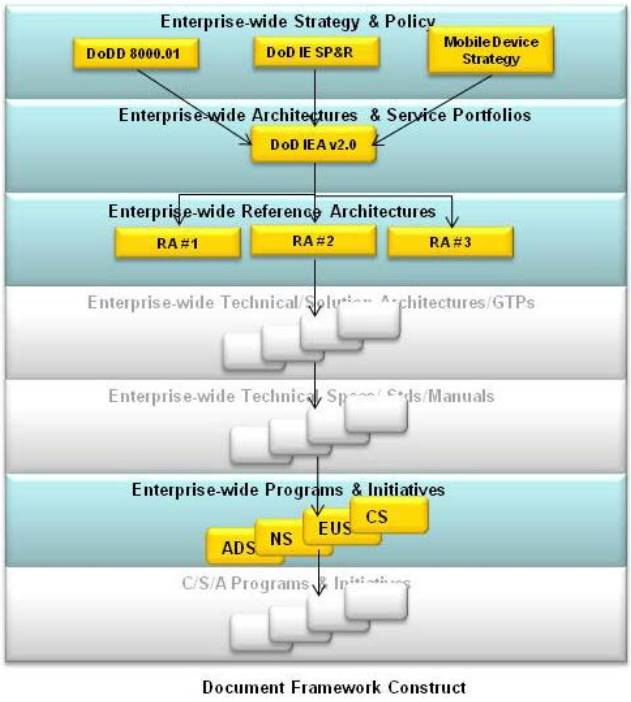


Figure D-4 - Position of RAs in Providing Solution Guidance

3.3 Process for Developing DoD Architectures Aligned with DoD IEA

This sub-section describes a high-level process for developing architectures so they align with the DoD IEA. The process describes how the DoD IEA should be used to shape architectures so they correctly reflect pertinent characteristics of the "to be" IE. It is not a "step-by-step" guide for building fully aligned views. Instead, it identifies what an architect needs to know about operations and information sharing in the IE and then how to apply that knowledge in developing and maintaining architecture descriptions aligned with the DoD IEA.

Figure D-5 shows the alignment process. While the DoD IEA content involved in this alignment can take several forms, depending upon the particular type of architecture under development and its purpose and scope, the basic process for accomplishing the alignment, regardless of architecture, is essentially the same. While the type of architecture being built may dictate the content being applied from the DoD IEA or the architecture views that result, the basics of what needs to be done to accomplish the alignment will not differ substantially. An example of how Mission Area architectures can be developed using the DoD IEA can be found in the Use Case: Mission Area Architect Use of the DoD IEA in Appendix I. A similar example of developing a Component architecture using the DoD IEA can be found in the Use Case: Component Architect Use of the DoD IEA in Section 5.2.3 also in Appendix I.

3.3.1 Understand the IE

The process starts with the architect carefully reviewing the DoD IEA. The purpose of this review is two-fold; to gain an understanding of the IE and its requirements, and to know what architecture information the IEA has and how it uses that information in describing the IE. The review should, at a minimum, cover operational requirements and context for the IE, vision of the desired IE end-state, and capabilities the IE must achieve, since these are key areas with which the architecture will need to align.

A comprehensive review of the IEA in this way gives the architect a basic understanding of how the IE is expected to be configured and operated. It also provides required knowledge of the IEA components with which the architecture under development will need to align. At a minimum, the review requires reading through the architecture description document. In addition, the architect may also want to review collected architecture data and developed architecture views in their native tool format to gain additional detail, enhance understanding, and enable a more complete analysis of alignment requirements.

With the IEA review completed, the architect will then be able to determine how the proposed architecture may need to use, operate in, and interact with the IE. This sub-step provides a starting point for determining the pertinent areas in the IEA with which the architecture will need to align.

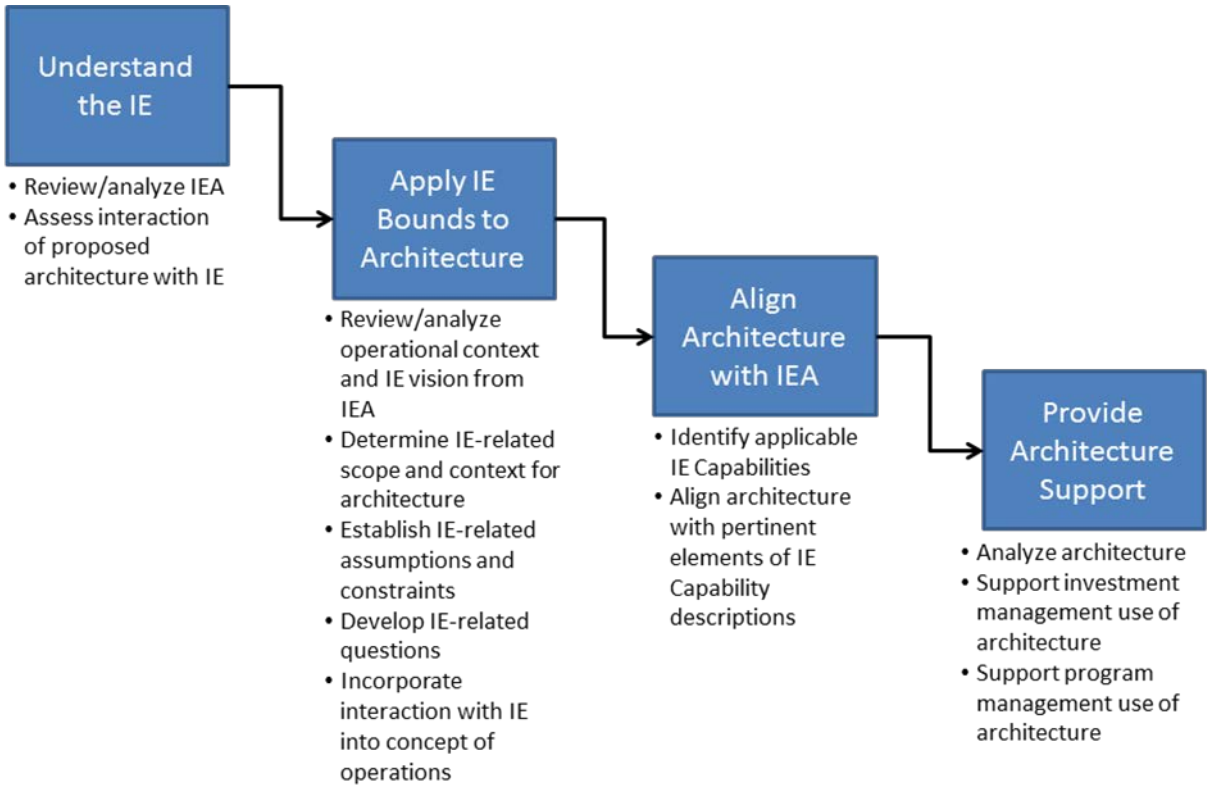


Figure D-5 – High-Level Process for Aligning Architectures to DoD IEA

3.3.2 Apply IE Bounds to Architecture

The next major step in the architecture alignment process focuses on using the proper DoD IEA content to put bounds on the architecture prior to development. This process step starts with a thorough review of the operational context from the DoD IEA to determine the requirements warfighter, business, and defense intelligence operators have for the IE and to establish how those requirements, as incorporated into the DoD IEA, apply to the architecture to be developed. This analysis should be combined with an evaluation of the IE vision describing the technical aspects of the desired end-state for the IE; this description complements the requirements discussion by providing a view of the technical characteristics of the IE that are required to be in place to enable the requirements established in the operational context.

With completion of a more detailed evaluation of these two key areas of the DoD IEA, the architect can then determine how the architecture to be developed fits within and should address the requirements of both the operator and the IE itself. This determination forms the basis for development of IE-related aspects of both the scope and context that guide architecture development. The IE aspects of the architecture's scope and context should be captured in pertinent areas of the architecture's AV-1 (Overview and Summary Information) so they properly guide architecture development and ensure the capture of correct aspects of the DoD IEA into the architecture where it needs to interact with the IE.

Boundaries for the architecture are also established by the assumptions and constraints integral to the architecture and the questions it is expected to answer. Based on the previously completed assessment of the operational context and IE vision from the DoD IEA, the architect should establish any necessary IE-related assumptions and constraints and capture these in the AV-1. An important part of determining IE-related scope for the architecture also involves development of IE-related questions that the architecture is expected to answer. These questions should also be incorporated into the AV-1 to be used to ensure collection of the proper information for incorporation into the architecture and to guide architecture analyses.

In addition to these scoping elements, a concept of operations is also developed as a starting point to guide architecture development. This concept of operations describes the mission, class of mission, or scenario governing the architecture. It describes the main operational concepts and interesting or unique aspects of operations that accomplish this mission. It also describes interactions between the subject architecture and its environment, and between the architecture and external systems. The operational concept provides a summary of what the architecture is about and an idea of the players and actions involved. This concept of operations is normally summarized in an OV-1 (High-Level Operational Concept Graphic) which depicts the mission or scenario, key players, and operation being performed.

To ensure the architecture can drive solutions able to effectively operate in the IE, it is important for the operational concept developed for any architecture interacting with the IE to properly incorporate pertinent aspects of the operational context and IE vision from the DoD IEA. The

architecture's concept of operations should describe how the architecture is to interact with the IE to successfully complete the mission. It should address how the IE enables the depicted operations. The role of key IE actions and performers, particularly enterprise services described in the DoD IEA, should be discussed in relation to accomplishing the mission or scenario described in the concept of operations. The IE and key interactions should be depicted prominently and correctly in any OV-1 developed for the architecture.

3.3.3 Align Architecture with the IEA

With the proper architecture scope and boundaries established and related to the IE, the architect can develop the architecture so it is in alignment with the DoD IEA. This involves using the information in the DoD IEA as a starting point for the architecture, incorporating and/or enhancing and refining this information as necessary. This process step begins with the architect selecting the IE capabilities that apply to the architecture under development. The selected IE capabilities and how they should be addressed in the architecture is dependent upon the relationship of the architecture to the IE, also called the architecture's perspective of the IE.

The following are the three main perspectives an architecture can take of the IE:

- Provider – the architecture describes the provision of key aspects of the IE and its infrastructure to meet operational requirements
- Manager/Operator – the architecture describes management and/or operation of key aspects of the IE to meet operational requirements
- Consumer/User – the architecture describes use of the IE for successful mission accomplishment

The architect uses the identified purpose and scope of the architecture, along with the IE-aligned assumptions, constraints, and concept of operations previously developed, to determine which of these perspectives apply. It must be noted that any given architecture description may address more than one of these perspectives and the perspective of the architecture itself may be different at different places in the architecture description. The architect then determines the IE capabilities applicable to the architecture under development based on the perspective(s) the architecture is determined to have the following:

- For the provider perspective of the IE, the architect identifies whole or partial IE capabilities the architecture will achieve for the IE.
- For the Manager/Operator perspective of the IE, the architect identifies whole or partial IE capabilities enabling management/operation of the IE, as well as any whole or partial IE capabilities the architecture is expected to specifically or uniquely manage/operate.

- For the Consumer/User perspective of the IE, the architect identifies whole or partial IE capabilities enabling the architecture to effectively accomplish its concept of operations.

Once IE capabilities applicable to the architecture have been identified, the architect can then use the descriptions of these capabilities from the DoD IEA, to include the descriptions of activities, rules, and services aligned with them, to properly describe in the architecture how it needs to interact with the IE. In particular, the architect should use the descriptions of the identified capabilities to define what the IE will provide or do for the architecture. The architect should then use the activities associated with each capability to describe actions that must be taken to achieve the capability, services associated with the capability to define what is needed to perform the activities, and rules associated with each capability to constrain how the activities are performed and the services operate in achieving identified capabilities.

3.3.3.1 Applying IE Capabilities to Architecture

For IE capabilities selected to address the provider perspective, the architect needs to consider the descriptions of these capabilities as prescriptive for the architecture. As the approved definitions of what an IE capability must provide or do, the information associated with each of the capabilities selected for this perspective provides requirements the architecture must address in achieving the capabilities for the IE. The architect can incorporate these capabilities into the architecture and then enhance, extend, or refine the accompanying capability descriptions, providing more detail as necessary to ensure proper solution development and implementation. However, these more detailed descriptions must remain true to how these capabilities are described in the DoD IEA.

For IE capabilities selected to address the Manager/Operator perspective, the architect also needs to consider the descriptions of capabilities that enable the architecture to manage and operate the IE as prescriptive for the architecture since these capabilities represent things the IE must do to ensure effective management and operation. For this reason, they represent IE requirements the architecture needs to fulfill, just as with the provider perspective. As before, the architect can incorporate, then enhance, extend, or refine the descriptions associated with selected IE capabilities, as needed, but the resulting detailed descriptions must again remain true to how these capabilities are described in the DoD IEA.

The IE capabilities selected because they represent things the architecture will uniquely manage or operate within the IE, on the other hand, impact the architecture indirectly. The IE capabilities selected for this reason should be applied to the architecture as constraints. Rather than their requirements being directly incorporated into the architecture, those requirements need to be converted into descriptions of how the capability should be managed and operated to meet its requirements.

For IE capabilities selected to address the consumer/user perspective, the architect needs to determine what the architecture must do to take advantage of these capabilities. The selected IE

capabilities are analyzed to determine how the architecture needs to interact with them in achieving its concept of operations. The descriptions of the selected IE capabilities provide constraints on how these interactions will occur, constraints which again need to be described in the architecture. They further establish requirements the architecture must address in order to best use the IE capabilities as they are achieved.

3.3.3.2 Applying Operational Activities from the DoD IEA to the Architecture

Once IE capabilities related to the architecture have been identified, the architect then determines which of the DoD IEA activities linked to each capability are applicable to the architecture description, based on its purpose, scope, and operational context. The architect also needs to determine how to apply the selected DoD IEA activities in the architecture under development. This representation depends upon the perspective the architecture takes of the IE in regards to the activity or process being described. Where the architecture is describing the provider or manager/operator perspective, the pertinent operational activities and processes in the architecture description should be directly derived from applicable DoD IEA activities. There are a number of ways to accomplish this:

- Incorporate actual DoD IEA activities (both names and definitions) directly into the architecture description
- Develop architecture activities as specific instances of the more generic DoD IEA activities
- Develop activities in the architecture description as decompositions ("drill downs") of existing DoD IEA activities, providing the additional level of detail needed to address the architecture's purpose, viewpoint, and scope

Where the architecture is describing use of the IE, the architect needs to relate applicable DoD IEA activities to operational activities and processes in the architecture description to show how these activities and processes use the DoD IEA activities in accessing and consuming data and services.

- In the case of process models, DoD IEA activities could be shown in process flows, linked or mapped to process steps, or assembled into sub-processes to show they are performed as integral parts of the process.
- In the case of activity models, the names of DoD IEA activities could be included in the descriptions of architecture activities, incorporating them as tasks performed to complete the activity.
- The DoD IEA activities could also be linked or mapped to architecture activities using a table in the architecture description to illustrate which DoD IEA activities are accomplished in completing the linked architecture activity.

In all cases, the DoD IEA activities should be used to refine, extend, or constrain descriptions of architecture activities and/or processes so they are consistent with the requirements of the IE, as described in the DoD IEA.

3.3.3.3 Applying Principles and Rules from the DoD IEA to the Architecture

Principles and rules defined in the DoD IEA are designed to drive common solutions and promote consistency and integration across DoD's key programs, applications, and services. As such, they should be applied to the operational and service descriptions contained in architectures to ensure resulting capability and service definitions reflect requirements from and are consistent with the description of the IE contained in the DoD IEA. The architect can determine which principles and rules are applicable to the architecture by analyzing which are linked to each of the IE capabilities being applied to the architecture under development.

It must be noted here that since Data & Services Deployment Business Rules (DSDR) 12 mandates the use of available Mandatory Core Designated DoD Enterprise Services, as described in Appendix G, regardless of the capability being delivered, this rule applies, regardless of the architecture being developed. No capability comparable to the Mandatory Core Designated DoD Enterprise Services should be developed unless there is a waiver granted by the DoD CIO. The architect needs to identify the subset of available Mandatory Core Designated DoD Enterprise Services that meet the architecture's specific requirements and describe the use of those applicable Enterprise Services in the architecture description. If there is a compelling operational need or business case to develop, modify, or sustain capabilities comparable to the available Designated DoD Enterprise Services, it needs to be well documented in the architecture description. Adherence to this rule promotes interoperability and reduces cost by driving the global use of common DoD-wide capabilities.

There are numerous ways to apply the DoD IEA principles and rules as constraints in an architecture description. The following paragraphs contain examples of three different approaches. These examples are not all inclusive nor should they be considered the only valid solutions.

- **Incorporate DoD IEA principles or rules into activity, process, and/or service definitions in the architecture description** – Selected DoD IEA principle and rule statements could be incorporated directly into the definitions of activities, processes, or services in the architecture description. In this way, these statements become an integral part of the description of how an action, process, or service operates, limiting these descriptions to boundaries imposed by the DoD IEA principle or rule.

- **Include DoD IEA rules in an architecture rules model** – How an architecture behaves may be described using a rules model. An architecture rules model contains statements of the conditions and standards governing the execution of activities, processes, and services described in the architecture. The rules in the model are connected to the

architecture objects they govern in different ways, depending upon the architecture development method and modeling approach and notation employed. For example, with the IDEF0 activity modeling convention, rules can be shown as controls on activities, imparting constraints on such things as the number and type of inputs needed to accomplish the activity, how the activity behaves in a given situation, and the outputs it will produce given certain conditions. Placing applicable DoD IEA rules into a rules model as part of the architecture description will effectively constrain architecture elements to behave according to the restrictions and requirements defined by the DoD IEA, allowing the resulting capabilities to effectively operate in the IE.

- **Use DoD IEA rules as the basis for more detailed restrictions to regulate solutions** – The DoD IEA rules can also be used as a baseline for developing more detailed restrictions to limit solutions developed, acquired, and/or deployed to meet architecture requirements. Services enabling or supporting activities or processes must abide by the restrictions imposed by the DoD IEA rules applicable to those activities or processes. These rules could be used as the starting point for deriving more detailed technical rules for regulating system design and/or analysis to ensure the resulting services exhibit the correct functionality and so are capable of operating in the IE. Since DoD IEA rules primarily focus on providing an effective IE to support operations, they are most useful in restricting the provision and management of data and services. However, they can also be indirectly applied to limit architecture solutions so they use data and services in the "right" way.

3.3.3.4 Applying Service Descriptions from the DoD IEA to the Architecture

The IE services described in the DoD IEA are enterprise services provided by a DoD-level entity for use by all or a large segment of the DoD user population or by a Military Department that are or can be used by other Military Departments. Such services perform functions derived from aligned activities to achieve IE capabilities. Each of the IE services described in the DoD IEA is expected to be delivered by one or more solutions combining Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Policy (DOTMLPF-P) elements. IE services are aligned with each of the IE capabilities described in the DoD IEA to represent the services considered necessary to achieve that capability.

The architect uses the descriptions of IE service aligned with applicable IE capabilities from the DoD IEA as the basis for defining the services that solutions driven by or resulting from the architecture under development are required to deliver. For architectures with a provider or manager/operator perspective of the IE, the descriptions of those services the architecture will deliver to the IE for achieving identified IE capabilities should be incorporated directly into the architecture description. These service descriptions can be extended, enhanced, and/or refined to provide the level of detail needed to meet the architecture's purpose, viewpoint, and scope, as well as to drive solution definition and implementation. The more detailed architecture

description of these services that results must, however, remain within the bounds set by the IE service descriptions in the DoD IEA.

For architectures with a manager/operator perspective of the IE that have identified specific IE capabilities to be managed/operated, the service descriptions from the DoD IEA that are aligned with those capabilities provide additional detail regarding what is to be managed/operated in achieving the capabilities. The architect should use these service descriptions, then, to better understand what the architecture must do to effectively manage/operate such services, and ensure the architecture description addresses the requirements associated with this necessary management/operation.

For architectures with a consumer/user perspective of the IE, the IE service descriptions aligned to IE capabilities with which the architecture needs to interact should be used to better understand what these interactions need to be and how they need to occur. This understanding should then be applied to the architecture under development in more completely describing use of the IE. The IE service descriptions provide the architect with additional detail to apply to the architecture in the form of constraints governing those actions and processes directly using the IE.

3.3.4 Provide Architecture Support

Once the architecture description has been developed and properly aligned with the DoD IEA, the architect supports its use in achieving the desired IE capabilities by developing, acquiring, and implementing required solutions. How architecture information is used depends upon the architecture type. Mission Area enterprise architectures are used primarily to direct IT transformation and support effective investment decision-making and management. Component enterprise architectures turn DoD guidance, policy, and investment decisions into means for achieving desired capabilities to enable effective warfighting, business, and defense intelligence operations. Solution architectures model the solutions and drive the programs needed to field the actual data and services necessary to achieve required IE capabilities.

For all these architectures, the architect works with users to analyze the architecture and answer key questions supporting required decisions. These questions should be framed by stakeholders prior to architecture development and become integral to the architecture's purpose. Their answers provide stakeholders with critical information needed for deciding on investments and programs. These questions will vary according to architecture purpose, viewpoint, and scope, as well as stakeholder needs. The architect also assists stakeholders in applying the results of architecture analysis, in conjunction with the contents of the architecture description, in support of developing, acquiring, and deploying the right data and services to meet mission needs.

3.3.4.1 Analyze Architecture

This process step begins with the conduct of an analysis of the contents of an architecture aligned with the DoD IEA to answer key questions for transformation and investment decision-making

and program management. Such analyses should involve not just the architect, but also supported decision-makers, portfolio managers, program managers, engineers, and integrators. In fact, to properly scope the architecture, this set of analysis stakeholders should be involved prior to architecture development in defining the types of analyses required and the information those analyses must provide.[13] Upon architecture completion, the analysis stakeholders should be involved in planning the subsequent analysis, to include determining the extent of that analysis and the questions it must answer. They should then work together to conduct the actual analysis – reviewing architecture information, determining what that information means for each of them, extracting the information needed to answer the posed questions, and then assessing the extracted information to draw conclusions regarding the capabilities needed to operate in the DoD IE in achieving net-centric information sharing.

Two types of analysis are of special importance to decision-makers and program managers. These analyses are:

- **Gap Analysis** compares the current IT environment with requirements established by the architecture to assess how well those requirements can be met with existing capabilities. The resulting IT "gaps," along with corresponding IT "redundancies" and "dead-ends," represent issues for which the decision-maker and/or program manager must provide resolutions to meet goals and objectives for the IE. The architecture provides the basis for prioritizing identified issues based on their impact on operations and mission accomplishment. Issues identified and prioritized in this way can be used to establish programs and initiatives for actually filling identified gaps and correcting identified redundancies and dead-ends and to guide architecture development to address critical mission needs.

- **Management Analysis** involves use of the architecture description in developing more detailed guidelines for managing investments and programs to meet goals and objectives for the IE and, most importantly, follow policy and guidance. This analysis uses the DoD IEA rules, as applied in the supporting architecture, as a starting point for developing more focused rules providing the level of detail needed to actually manage the acquisition of capabilities defined by the architecture. These more detailed rules are extensions, refinements, and/or enhancements of applicable DoD IEA rules. They should be applied by decision-makers and program managers in directing portfolios and programs and as the basis for selecting solutions to meet established needs.

3.3.4.2 Support Use of Architecture

The architect then works with architecture stakeholders to support proper use of the architecture and architecture analyses in achieving required IE capabilities. Once properly aligned with the

[13] The list of required analyses is then used in planning the architecture and its development and should be captured in the architecture's overview and summary information.

DoD IEA, the architecture can be effectively used to align portfolios and/or programs with requirements from the DoD IEA. Because of the importance of investment and program management use of architectures, the next two sections focus on how an architecture, properly aligned with the DoD IEA, could be used to enable the actions of portfolio managers, IRBs, and PEOs/PMs.

4 Use of DoD IEA in Investment Decision-Making

Managing IT investments involves strategic planning for determining and governing the application of scarce monetary resources to acquire, maintain, and operate an optimal mix of IT services for accomplishing the operational objectives of an enterprise. In DoD, this management function involves two processes. The IT Portfolio Management (PfM) process uses integrated strategic planning, integrated architectures, measures of performance, risk management techniques, transition plans, and portfolio investment strategies to oversee and govern selected groupings of IT investments. The IT Investment Review process complements and supports PfM by converting transition plans into implementation plans for the portfolio, certifying that programs and initiatives meet portfolio objectives, and recommending the approval of funds for programs and initiatives based on their contribution to the portfolio. The following sub-sections describe how the DoD IEA, as applied in supporting architectures, can provide portfolio managers and IRBs with the means to make informed decisions regarding IT investments. These descriptions are meant to complement the Use Cases IEA Support to Transition Planning and IEA Support to Investment Planning found in Volume I of the DoD IEA description. These descriptions are meant to complement the Use Cases: IEA Support to Transition Planning and IEA Support to Investment Planning found in Appendix I.

4.1 IT Portfolio Manager Use of DoD IEA

Proper execution of IT PfM requires portfolio managers to have the information necessary to make informed decisions regarding investments in IE capabilities. Architects and PEOs/PMs provide this information. Consequently, both architects and PMs must ensure the information they provide has been properly aligned with the DoD IEA to enable informed decisions in support of achieving required IE capabilities. In developing the architectures governing a given portfolio, primarily MA EAs and related capability architectures and RAs, the architect should have properly scoped and bounded the governing architectures through development of IE-related assumptions, constraints, and questions, and a concept of operations describing required interaction with the IE. The architect should also have incorporated descriptions of pertinent IE capabilities and associated activities, rules, and services from the DoD IEA into governing architectures and extended, enhanced, and/or refined these descriptions, as necessary.

IT portfolio management involves identification, selection, control, and evaluation of information resources. How DoD IEA-aligned architecture descriptions would be used to enable each of these functions is described in the sub-sections that follow.

4.1.1 Identification

In identification, the scope of the IT portfolio and its investments are determined. Portfolio objectives are derived from, and linked to, the vision, mission, goals, objectives, and priorities of the enterprise. During identification, the portfolio manager also performs the following:

- Identifies capability gaps, opportunities, and redundancies for the portfolio
- Determines investment risks
- Plans for continuous process improvement
- Develops quantifiable, outcome-based performance measures for use in tracking and grading investment decisions

The IT portfolio manager can use relevant governing architectures aligned with the DoD IEA to provide portfolio objectives based on the Department's IE vision and derived from the required IE capabilities. The IE capability descriptions, as applied in these architectures, provide requirements for the capabilities the portfolio must either develop or that support the portfolio in implementing solutions able to operate in the IE. The operational context and IE vision from the DoD IEA, as incorporated into the governing architectures, allows the construction of portfolio objectives reflecting these requirements. Each portfolio manager should focus investment planning toward the IE capabilities as aligned with the IE vision representing the desired IE end-state.

The IT portfolio manager can also use the descriptions of IE capabilities as incorporated into the governing architectures as a starting point for developing criteria for investment decision-making and to establish performance measures for tracking and grading those decisions. The portfolio manager can then use these criteria to assess the portfolio baseline to determine IE capability gaps, opportunities, and redundancies. A portfolio manager could further use the principles and rules aligned with selected IE capabilities, as described in supporting architectures aligned with the DoD IEA, to extend these criteria for use in assessing whether programs in the portfolio provide the necessary abilities (identify capability gaps and redundancies), and how investments should be adjusted to address resulting issues (identify opportunities, plan for continuous process improvement, and identify investment risks).

4.1.2 Selection

During selection, the portfolio manager establishes the optimal mix of IT investments to achieve the portfolio's goals and objectives within resource constraints, while demonstrating the impact of alternative IT investment strategies and funding levels on the portfolio and accomplishment of

the portfolio's portion of the desired IE end-state. The DoD IEA provides a common language and context for evaluating various investment strategies for the portfolio, as well as a basis for determining which investments provide the highest potential for meeting requirements established by IE capabilities aligned to the portfolio. Use of the IE capability descriptions from the DoD IEA, as applied to pertinent governing architectures, allows the portfolio manager to identify, compare, and evaluate very different capability investments to a common baseline in order to judge their ability to meet operational requirements for the IE and the IE vision established by the DoD IEA.

As part of the selection function, the portfolio manager measures potential solutions against criteria derived during identification from IE capability descriptions to establish whether those solutions should be part of the portfolio. Pros and cons can be identified for each solution based on its ability to meet requirements for the applicable IE capabilities and their associated activity, rule, and service descriptions. These measurements also provide data for use in adjusting the portfolio to provide the best mix of investments for enabling and implementing solutions able to meet operational needs.

4.1.3 Control

During control, the portfolio manager uses established, quantifiable, outcome-based performance measures to monitor and manage the actual investments in the portfolio as they are developed and implemented. Programs resulting from portfolio investments are evaluated against portfolio objectives with recommendations made to continue, modify, or terminate individual investments based on the results.

The portfolio manager uses criteria derived from applicable IE capability descriptions and associated principles and rules, as applied in the governing architectures, to determine whether programs can be expected to meet IE requirements and provide the necessary IE capabilities. The descriptions of applicable IE capabilities from governing architectures aligned with the DoD IEA provide a "picture" of what target capabilities should be and how they should perform for use in measuring investments and associated programs. The portfolio manager should use all these elements to determine the current state of the portfolio and then adjust its investments accordingly to better align them with requirements from the DoD IEA.

4.1.4 Evaluation

Periodically, the portfolio manager measures the actual contributions of fielded capabilities provided by the portfolio to the enablement of operations. The portfolio manager measures the actual support provided by the portfolio's investments against established, outcome-based performance measures to determine whether the portfolio is providing improved capability and where gaps still exist. The results of this evaluation are used to determine further adjustments to the portfolio and to repeat the identification function.

The governing architectures, aligned with the DoD IEA, provide the portfolio manager with a description of the IE vision and how IE capabilities operate in this environment for information sharing purposes. The portfolio manager uses the IE capability descriptions aligned to the portfolio to establish criteria for measuring whether the portfolio is delivering the right capabilities and/or whether the capabilities it is providing are working so as to enable operations. The DoD IEA, as interpreted by the governing architectures, can be used as a target, since it provides a view of how the "to be" IE is expected to operate. The portfolio manager can compare the current state and performance of the IE against this target to see if the portfolio has actually advanced the IE towards the desired end-state. Investments can be reviewed and adjusted, as necessary, to better meet the requirements of IE capabilities described in the governing architectures as aligned with the DoD IEA.

4.2 Investment Review Board (IRB) Use of DoD IEA

The IT Investment Review process complements and supports IT PfM. The IRB will certify programs and initiatives that meet portfolio objectives and then will approve funding for certified programs and initiatives. The IRB process and structure was first established in DoD to meet directives in the National Defense Authorization Act of Fiscal Year 2005 (FY05 NDAA), which mandated certification of DoD business systems modernization programs. To conform to these directives, DoD established a governance structure, roles, responsibilities, and processes for conducting the necessary business system certification. This process is considered the *de facto* standard for investment review across the Department.

The IRB will receive requests for certification of programs and initiatives as part of transition plans for the IE. The PMs for the programs and initiatives are responsible for assembling certification packages containing accurate and complete information on their programs to include how they address DoD IEA requirements and portfolio goals and objectives. Pre-Certification Authorities (PCAs), appointed by the Components, review and validate the certification packages, then submit them to the IRB for certification review and recommendation. The IRB checks the programs and initiatives against portfolio goals and objectives and DoD IEA-established requirements and submits programs they recommend for certification to a designated Certification Authority (CA) at the Principal Staff Assistant (PSA) level for final approval. If approved, funds are formally obligated for the program/initiative.

The DoD IEA describes a common vision for the IE in terms of IE capability descriptions that provide a basis for certification criteria to be used by the IRB for making decisions regarding IT programs/initiatives and their place in IT portfolios. The IE capability descriptions from the DoD IEA can also be used to locate commonalities across programs and initiatives for the IRB to use in eliminating redundancies and promoting program reuse across the Department. Since the DoD IEA defines the target end-state for the IE, it can be used as a baseline to determine if a program/initiative is advancing towards the Department's IE goals and so is aligned with DoD's

needs in regards to future operations. All these factors will determine if a program/initiative should be certified and ultimately funded.

To properly conduct its assessment of a program/initiative, the IRB needs to receive information from both portfolio managers and PEOs/PMs with a stake in the program/initiative under review. From portfolio managers, the IRB needs to receive IE capability requirements associated with the portfolio. This information would be drawn from governing architectures aligned with the DoD IEA. The IRB can then review the program/initiative against this information to assess its compliance or alignment with the vision for the IE.

From PEO(s)/PM(s), the IRB would receive assertions as to how the program/initiative complies with IE requirements. These assertions are based on how the solution architecture(s) governing the program align with the DoD IEA. The solution architect first incorporates into the solution architecture those applicable IE capability descriptions, to include associated activities, rules, and services, as interpreted by any governing architecture(s). The solution architect also addresses additional requirements defined by applicable DoD-wide RAs that are a part of the DoD IEA in defining solution requirements and providing detailed technical standards and rules for directing solution development. The PEO/PM describes for the IRB the IE-related descriptions and requirements from the solution architecture and RAs with which the program is compliant. The IRB then assesses how this interpretation aligns with the DoD IEA.

The IRB should conduct its assessments using criteria derived from the DoD IEA to determine program/initiative compliance. The IRB should use applicable IE capability descriptions, as extended by the associated activity, rule, and service descriptions, to determine the requirements the program/initiative should be addressing. The applicable IE capability descriptions as integrated into governing architectures can provide the IRB with a common context for understanding how the program/initiative can expect to operate in the "to be" IE. This context can be used to develop measures for determining how well the program/initiative is to perform in such an environment.

5 Use of the DoD IEA in Program Management

This section describes how PEOs/PMs should use solution architectures, properly aligned with the DoD IEA, in carrying out their responsibilities. Program Executive Officers and PMs are the designated individuals with responsibility for program development, production, and sustainment to meet users' operational needs. In particular, PMs are a focal point for providing decision-makers with information on Programs of Record (PoRs) and how these PoRs meet IE requirements. As such, PMs are responsible for ensuring that all required data on their PoRs provide an accurate picture, in the context of the IE, of the state of the program to enable their Component organizations, as well as DoD portfolio managers, IRBs, and the DoD CIO, to make informed investment decisions.

The solution architecture for the program should be derived from and compliant with appropriate higher-level architectures. These governing architectures provide the solution architect with an operational concept the program must follow, a set of capabilities it must achieve, a set of higher-activities the program must support, descriptions of required services the program is to provide, and additional guidelines to which the program must adhere. These governing architectures are assumed to have been aligned with the DoD IEA.

In developing a solution architecture, the architect should have taken into consideration pertinent DoD IEA descriptions as applied by the governing architectures. The governing architectures will have incorporated and extended, enhanced, or refined, where applicable, the descriptions of pertinent IE capabilities and their associated activities, rules, and services from the DoD IEA. The solution architect then incorporates these descriptions into the solution architecture, further extending, enhancing, or refining them to meet development needs. The PEO/PM will use the operational processes, service requirements, rules, and standards from the solution architecture to manage the program and select solutions to meet program needs by deriving IE-related non-functional requirements, design criteria and guidelines, and criteria for analyzing alternatives.

The appropriate timeframe to start aligning with DoD IEA requirements is during the Capabilities Based Assessment (CBA) phase of the Joint Capabilities Integration and Development System (JCIDS) process.[14] The CBA sets the stage for subsequent acquisition. Before initiating a program, the CBA identifies warfighting capability and supportability gaps and the DOTMLPF-P elements required to fill those gaps. The solution architecture, aligned with the DoD IEA, should be a key source for this gap analysis and also for determining appropriate IE capabilities to which the solution should be built in order to fill the identified gaps. Because the Initial Capabilities Document (ICD) developed during the CBA provides the formal means for communicating capability needs between the warfighter, acquisition, and resource management communities, it must incorporate appropriate DoD IEA elements, as interpreted by governing architectures and the solution architecture, in defining IE-related aspects of the program.

Evolutionary acquisition is the preferred DoD strategy for rapid acquisition of mature technology for the user. An evolutionary approach delivers capability in increments, recognizing, up front, the need for future capability improvements. The objective is to balance needs and available capability with resources, and to put capability into the hands of the user quickly. The success of the strategy depends on phased definition of capability needs and system requirements, and the maturation of technologies that lead to disciplined development and production of systems that provide increasing capability over time.[15]

In support of evolutionary acquisition, the IE vision in the DoD IEA, as applied by higher-level governing and solution architectures, can assist in determining transformation priorities the

[14] CJCSI 3170.01G, 1 March 2009, Current as of 7 March 2011
[15] DoDI 5000.02, Dec 8, 2008, p. 13

PEO/PM can use to decide which capabilities should be developed and/or acquired first. This common IE vision, as incorporated into the applicable solution architecture(s), can also be used to determine the required end-state of IE capabilities to be provided by the program. The IE capability descriptions, as constrained by associated rules, can be used to establish criteria for assessing the current position of the program in meeting IE requirements and for planning future improvements and defining incremental development goals to address requirement gaps.

Appendix E: Compliance with the DoD Information Enterprise Architecture (DoD IEA)

1 Introduction

Compliance with the Department of Defense (DoD) Information Enterprise Architecture (IEA) is a necessary first step to ensure components of the IE operate and interoperate as planned. Architectures are responsible for maintaining compliance with the IEA as purposes and scopes change. As IE goals and capabilities change, content in the IEA will be revised to reflect these changes. Architectures must determine how best to keep up with the IEA as it is revised. Appendix E describes the criteria for complying with the DoD IEA. It also contains a template that can be used to assist in conveying and assessing compliance with the IEA. *Appendix D, Applying the DoD IEA*, is a complementary appendix that should be read and understood before reading this appendix. Appendix D describes a detailed approach for developing DoD architectures that comply with the DoD IEA and how these compliant architectures can be used to support the functions of IT investment managers and managers of Information Technology (IT) programs.

1.1 Related Compliance Requirements

Conformance with the DoD Architecture Framework (DoDAF) and compliance with the DoD Enterprise Architecture (EA) are closely related to compliance with the IEA. DoD architectures are expected to meet compliance requirements in all three areas. Certain organizations, such as the US Special Operations Command, with unique legal, operational, and organizational considerations may not be impacted by the DoD IEA.

DoDAF conformance ensures that reuse of information, architecture artifacts, models, and viewpoints can be shared with common understanding. DoDAF conformance is achieved when the data in a described architecture is defined according to the Meta Model (DM2) concepts, associations, and attributes and the architectural data is capable of transfer in accordance with the Physical Exchange Specification (PES). Information on conformance with the DoDAF is described in the DoDAF v2.0 document.

DoD IEA compliance is one of many components required for compliance with the DoD EA. Information about compliance with the DoD EA is provided in Appendix G of this document.

1.2 Importance of Relevance

In most cases, compliance is a function of determining what information in the IEA has relevance for the architecture being developed. Relevance is based on the purpose and scope of the architecture. An architecture with a purpose and scope that requires high-level, general descriptions, such as an EA, may determine the operational context, vision, and principles of the IEA as being relevant for compliance. An architecture with a purpose and scope that requires focused, detailed descriptions, such as a Reference Architecture or Solution Architecture, may

determine the capabilities, activities, rules, and services of the IEA as relevant for compliance. DoD IEA compliance for any architecture is based on the purpose and scope of the architecture.

2 Compliance Criteria

Various elements described in the IEA will be used to establish compliance criteria. Compliance with the DoD IEA will be evaluated using this criteria based on relevance to the architecture. The intent of Appendix E is to provide information for complying with the DoD IEA content. Although IDEF0 examples are used in this section, the focus is on the DoD IEA content not the IDEF0 rules and disciplines.

2.1 Align with Operational Context

The operational context describes the operational requirements and desired mission outcomes the IE must enable and support. These requirements and outcomes are established by the warfighting, business, defense intelligence, and enterprise information environment Mission Areas. Information about the operational context is in Section 2 of this document.

Guidance that scopes and bounds the architecture should be aligned with the DoD IEA operational context so the architecture properly addresses warfighter, business, and defense intelligence needs for the IE. This alignment may be conveyed in the Overview and Summary Document (AV-1) and external context descriptions.

2.2 Align with IE Vision

The vision for the IE is a unified environment that delivers agile and secure information capabilities to enhance combat power and decision making. The IE provides a rich information sharing environment in which data and services are visible, accessible, understandable, and trusted across the enterprise. It also enables an available and protected network infrastructure that enables responsive, information-centric operations, using dynamic and interoperable communications and computing capabilities. Information about the IE vision is in Section 4 of this document.

Architecture guidance should also be aligned with the vision describing the desired technical end-state of the IE so the architecture can guide development and implementation of solutions able to effectively operate in such an IE. This guidance should include an operational concept incorporating a description of how the architecture interacts with the IE, based again on the operational context and IE vision in the IEA. This alignment may be conveyed in the Overview and Summary Document (AV-1), the Vision (CV-1), and the Concept of Operation (OV-1).

2.3 Align with IEA Principles

The principles for the IE are the fundamental concepts for developing, operating, managing, and using the IE. The IE Operational Concept also fits in this criterion. The operational concept describes the key concepts, operations, components, and participants of the IE. It provides both a user and provider perspective. The principles are grouped by five priority areas and listed in Appendix B of this document. Information about the operational concept is in Section 6 of this document.

The application of principles can be expressed directly or indirectly in operational concepts. Enterprise-level architectures may incorporate the exact description of a principle from the DoD IEA into the OV-1 or they may only incorporate a portion based on the focus of the architecture. Data and Services Deployment (DSD) Principle 05 states *"Data, services, and applications should be loosely coupled to one another. The interfaces for mission services that an organization provides should be independent of the underlying implementation. Likewise, data has much greater value if it is visible, accessible, and understandable outside of the applications that might handle it."* The principle in its entirety may be expressed in the OV-1 or only a portion, such as *"Data, services, and applications should be loosely coupled to one another."* dependent upon the focus of the architecture.

The application of principles can also be expressed as an activity or within the definition of an activity in an OV-5 Operational Activity Model. A dynamic, agile, and responsive characteristic is present in several principles. These characteristics may be used to express the application of principles in an activity, or in the definition of an activity. **Table E2.3-1** provides an example of this using an activity from the Information Assurance (IA) Integrated Architecture.

Table E2.3-1 - Expressing Principles in Activities

Activity	**Definition**
IA Activity: A.3 Evolve the IA	Perform activities to analyze current IA capabilities as well as to define and plan new capabilities.
Example of Expressing a Principle in the Definition: A.3 Evolve the IA	Perform activities to analyze current IA capabilities as well as to define and plan new capabilities. The globalization of information technology, particularly the international nature of hardware and software (including supply chain) development and the rise of global providers of IT and communications services presents a very new and unique security challenge. GIG resources must be designed, managed, protected and defended to meet this challenge.

In Table E2.3-1, the activity and definition at the top of the table is an actual activity from the IA Global Information Grid (GIG) Integrated Architecture.[16] The activity, A.3 Evolve the IA, is defined as "Perform activities to analyze current IA capabilities as well as to define and plan new capabilities." The definition of the same activity at the bottom of the table includes the SA Principle 02 from the DoD IEA in blue text. By expressing SA Principle 02 in the definition, the intent and net-centric nature of the activity is more clearly articulated.

Another way to express the application of principles is as controls on activity and process models. Using Integrated Definition (IDEF) 0 modeling notation, the application of a Principle

[16] Information Assurance (IA) Component of the GIG Integrated Architecture, Increment 1, v1.1, 16 Nov 2006, pg. 3-25.

can be expressed as a Control directly on the activity. **Figure E2.3-1**, Expressing Principles as Controls on Activities, illustrates this method of expression.

In Figure E2.3-1, the activity in Block A expresses the application of principles by using the DSD Principle 05 as a control on the activity. DSD Principle 05 is defined as "*Data, services and applications must be visible, accessible, understandable, and trusted by the unanticipated user. All needs can never be fully anticipated. There will inevitably be unanticipated situations, unanticipated processes, and unanticipated partners. By building capabilities designed to support users outside of the expected set, the Department can achieve a measure of agility as a competitive advantage over our adversaries.*"

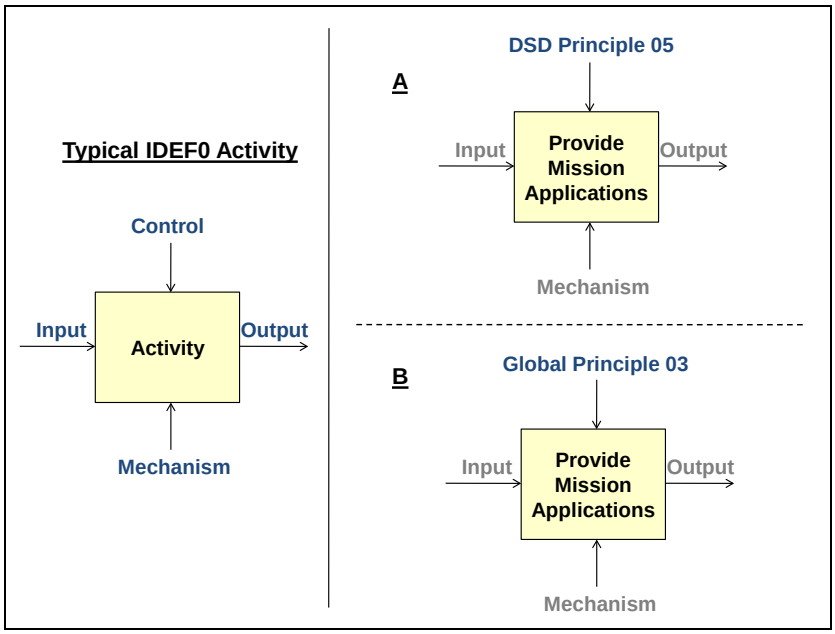


Figure E2.3-1: Expressing Principles as Controls on Activities

In this case, all elements of the principle will constrain the execution of the activity which may be further expressed in the definition or in processes involving the activity. In Block B, Global Principle 03 is used as a control on the activity. Global Principle 03 is defined as "Data assets, services, and applications on the GIG shall be visible, accessible, understandable, and trusted to authorized (including unanticipated) users." In this case, all elements of the principle will constrain the execution of the activity which may also be further expressed in the definition or in processes involving the activity.

2.4 Align with IEA Capabilities

The IE capabilities represent the functions required to securely consume, produce, and/or manage information and information assets within the IE. Together, these capabilities are meant to represent the totality of what the IE must be able to do or provide to enable successful mission accomplishment. In the DoD IEA, each IE capability is represented as an architecture description of the activities, functions/services, and rules that when implemented or executed can be expected to achieve the capability in terms of a measurable result. Information about the IE capabilities is in Section 5 of this document.

Capabilities described in the architecture should be aligned with pertinent IE capabilities described in the IEA. In cases where the architecture provides one or more IE capabilities, corresponding capability descriptions in the IEA should provide the starting point for more detailed capability descriptions in the architecture. Where IE capabilities from the IEA enable the architecture, the IEA descriptions of these capabilities should guide and constrain the corresponding capability descriptions in the architecture, providing information on where and how the IE capabilities will interact with the architecture and what they can be expected to provide in support. Application of capabilities may be conveyed in the Capability Taxonomy (CV-2) and other capability viewpoints.

2.4.1 Align with IEA Activities

The operational activities in the IEA represent the actions providers, users, and operators of the IE must perform to meet both operational requirements for the IE and the vision of the IE. Information about the IE operational activities is in Section 5 of this document.

Activities from the DoD IEA should be incorporated into the architecture or serve as starting points for further activity decomposition wherever the architecture needs to describe actions performed to achieve pertinent IE capabilities. They should also be incorporated into the architecture as necessary to constrain how actions or processes that need to occur in the IE are to be performed. Activities from the DoD IEA may also be used in the architecture to describe actions the IE will perform to enable or support the architecture and its interaction with the IE.

Operational activities and processes derived from relevant DoD IEA activities may be expressed in OV-5 Activity Models and process flows. This can be done by:

- Incorporating actual DoD IEA activities into the architecture description
- Developing architecture activities as specific instances of DoD IEA activities
- Developing architecture activities as decompositions of existing DoD IEA activities providing additional detail.

Figure E2.4.1-1, Examples for Expressing DoD IEA activities in the OV-5, provides three examples for expressing applicable DoD IEA activities in the OV-5. The figure uses DoD IEA Activity A1135-Develop Data/Service Standards as the applicable activity. The first example in the figure incorporates DoD IEA Activity A1135 Develop Data/Service Standards as activity A2 of the architecture's OV-5. The second example expresses the DoD IEA Activity A1135 as a specific instance to develop design patterns for ISR services in activity A2 of the architecture's OV-5. The third example provides additional detail with a decomposition of the DoD IEA Activity A1135 that fits the purpose of the architecture's OV-5.

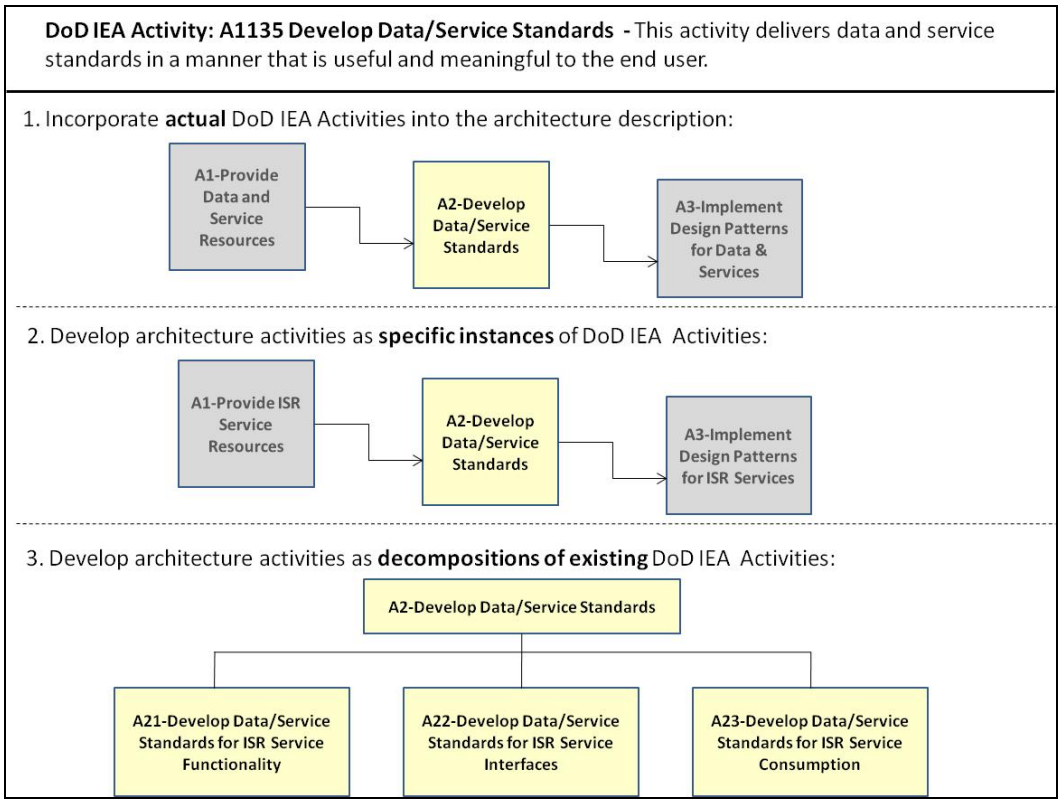


Figure E2.4.1-1: Examples for Expressing DoD IEA Activities in the OV-5

2.4.2 Align with IEA Services

The IE services represent the enterprise services and sub-services that are needed to deliver capabilities. Information about services and sub-services is in Section 7 of this document.

Services defined in the DoD IEA should provide the basis for descriptions of performers (services, systems, etc.) the architecture will provide to achieve IE capabilities. They also provide information for incorporation into the architecture to describe how IE services enable the architecture and how the architecture should interact with these enabling services.

Application of DoD IEA services may be conveyed in Services Context Descriptions (SvcV-1), Services Functionality Descriptions (SvcV-2), and other Service Viewpoints.

2.4.3 Align with IEA Rules

The IE rules represent the controls that are applied to activities and services. The rules are organized by five priority areas and the GIG 2.0 ORA-Derived Operational Rules (OPR) and associated directly to capabilities. Information about the rules is in Appendix B of this document.

Rules in the DoD IEA should be used to identify, select, and describe more detailed technical rules for incorporation into the architecture so it can properly constrain the implementation and functioning of solutions in ensuring effective operations in the IE.

The application of DoD IEA rules can be expressed in several ways to describe how the architecture operates. Three ways to express the rules in architecture descriptions are:

- In activity, process, and service definitions
- In architecture rules models
- As the basis for more detailed restrictions

Expressing the application of DoD IEA rules in activity, process, and service definitions provides descriptions of how an action, process, or service operates within the constraints of the Rule. The DSD Rule 07 states "Services shall be advertised by registering with an enterprise service registry." At enterprise and Component-level architectures, this rule can be expressed in the definition of activities in the OV-5. An example of expressing this Rule in a definition for implementing services is: The activity of activating services and making them available to users to include registering services with an enterprise service registry.

An architecture describing the process for implementing services may express the DSD Rule 07 by making "register with an enterprise service registry" a step in the process.

Expressing the application of DoD IEA rules in architecture rules models provides more descriptive content on how the architecture behaves. They effectively constrain architecture elements to behave according to the net-centric restrictions imposed by the DoD IEA Rule. Operational rules are specified in the OV-6a Operational rules Model to describe what must be done and what cannot be done in the enterprise. Operational rules can be grouped into three categories:[17]

- Structural Assertions - Concern mission or business domain terms and facts reflecting static aspects of business rules
- Action Assertions - Concern some dynamic aspects of the business and specify constraints on the results that actions produce
- Derivations - Concern algorithms used to compute a derivable fact based on other assertions

DSD Rule 05 states *"COIs will determine which data sources are authoritative and will not declare any source authoritative without establishing a valid pedigree."* As an example, this Rule can be expressed in the OV-6a as a structural assertion, action assertion, or derivation depending on architecture context and purpose.

- Structural Assertion - "Authoritative sources of data must have a valid pedigree."

[17] DoD Architecture Framework (DoDAF), v2, Viewpoints and Models, http://dodcio.defense.gov/sites/dodaf20/products/DoDAF_v2-02_web.pdf .

.

- Action Assertion - “Establish a valid pedigree for data sources before declaring them as authoritative.”Derivation - “Only data sources with valid pedigrees can be declared authoritative.”

Expressing the application of DoD IEA rules as the basis for more detailed restrictions uses the rules as a starting point for developing detailed technical rules. The technical rules are constraints on system and service performance and are typically addressed in the SV-10a Systems Rules Model and SvcV-10a Services Rules Model. In contrast to the OV-6a, SvcV-10a and SV-10a focus on constraints imposed by some aspect of operational performance requirements that translate into service and system performance requirements.18 CIR Rule 04 states “*Physical implementation of computing infrastructure shall include transparent interfaces to users to minimize, if not eliminate, degradation in performance and Quality of Service*.” An example of a detailed technical rule based on the CIR Rule 04 is “*Computing capabilities require intuitive management and use interactions to facilitate transparency.*”

2.4.4 Align with IEA Standards

The Standards for the IE assist in identifying applicable standards, guidance, and policy by listing existing and emerging documentation containing such information. Once identified, these standards are used to direct, guide, and/or constrain the execution of capabilities or services in the IE. Information about the Standards is in Section 8 of this document.

Standards in the DoD IEA should be used to identify, select, and describe more detailed specific technical standards for incorporation into the architecture so it can properly constrain the implementation and functioning of solutions in ensuring effective operations in the IE. Application of standards in the DoD IEA may be conveyed in the Standards Profile (StdV-1), Standards Forecast (SvcV-2), Services Evolution Description (SvcV-8), and Services Technology & Skills Forecast (SvcV-9) models.

2.5 Align with DoD-wide Reference Architecture (RA)

A DoD-wide Reference Architecture (RA) is an extension of the IEA that is scoped around some particular IEA functional or capability subset, adding depth to the IEA architectural description within that functional or capability subset.

As applicable, DoD architectures incorporate or align with the more detailed RA descriptions, and program planning, management, and execution uses appropriate RAs to provide standard solutions. DoD-wide RAs are just one element of a continuum of IE information ranging from enterprise-level policy and strategy to individual programs or initiatives that deliver or manage IE solutions. RAs are not typically implemented as a solution per se, but instead feed lower-level and more granular architectures, technical guidance, and programs. Since RAs describe the same architecture data as discussed earlier, only more focused and detailed, these descriptions can be applied as described earlier.

3 Compliance Template

The Compliance Template is a tool to assist architects with complying with the DoD IEA and evaluators with assessing architectures for compliance with the IEA. It lists the criteria for

[18] DoD Architecture Framework (DoDAF), v2, Viewpoints and Models, http://dodcio.defense.gov/sites/dodaf20/products/DoDAF_v2-02_web.pdf .

compliance and provides exemplar guidance for conveying compliance. The examples provided in this appendix use DoDAF architecture descriptions. Programs and portfolios that are not required to develop DoDAF architecture are expected to demonstrate compliance with the DoD IEA in whatever descriptions they provide. Documentation of compliance with the DoD IEA is expected regardless of the architecture description type. The Enhanced Information Support Plan (EISP) tool provides an automated means to use this template. The Compliance template is provided as Tab A to this Appendix.

Tab A to Appendix E: DoD IEA Compliance Template

Compliance Criteria	Appendix D Application Reference	Exemplars for Conveying Compliance	Questions to Address Compliance Criteria	Answers to Questions
2.1. Align with Operational Context	3.3.2 - Apply IEA Bounds to Architecture.	Review the Operational Context to determine which operational requirements apply to and bound the architecture being developed. Describe in the Overview and Summary Information (AV-1).	**Q** – Which warfighting, business, and defense intelligence operational requirements are relevant in bounding the architecture being developed? **Q** - Where in the architecture/ program documents are the relevant operational requirements described?	
2.2. Align with IE Vision	3.3.2 - Apply IEA Bounds to Architecture	Capture relevant conceptual and technical aspects of the IE Vision in the scope and context of the architecture. Describe in the Overview and Summary Information (AV-1).	**Q** – Which conceptual aspects of the IE Vision are relevant to my architecture? **Q** - Which technical aspects of the IE Vision are relevant to my architecture? **Q** - Where in the architecture/ program documents are the conceptual and technical aspects of the IE Vision described?	

Compliance Criteria	Appendix D Application Reference	Exemplars for Conveying Compliance	Questions to Address Compliance Criteria	Answers to Questions
2.3. Align with IEA Principles	3.3.3.3 - Apply relevant IEA Principles to drive common solutions and promote consistency and integration across DoD.	Identify relevant IEA Principles and apply in operational and service descriptions in the architecture being developed. Apply in the concepts of operations (OV-1), activity models (OV-5a), process models (OV-6c), and rules models (OV-6a, SvcV-10a)	**Q** - Which Priority Areas are relevant to the architecture being developed? **Q** – Which Principles from the relevant Priority Areas are relevant to the architecture? **Q** – How do these Principles apply to the architecture? **Q** - How are the Principles addressed in the architecture/ program documents?	
2.4. Align with IEA Capabilities	3.3.3.1 - Apply relevant IEA Capabilities and definitions to the architecture being developed as prescriptive, descriptive, or constraining content.	Based on the relevant IEA capabilities, describe what the IE will provide or do for the architecture and how the architecture will interact with the IE. Describe in the Capability Viewpoints, especially the Vision (CV-1) and Capability Taxonomy (CV-2); Operational Viewpoints, especially the Concept of Operations (OV-	**Q** – Which IEA Capabilities are relevant to the architecture being developed? **Q** – How do the Capabilities apply to the architecture? **Q** - Where in the architecture/ program documents are the relevant Capabilities applied?	

Compliance Criteria	Appendix D Application Reference	Exemplars for Conveying Compliance	Questions to Address Compliance Criteria	Answers to Questions
		1); and Services Viewpoints, especially the Services Context Description (SvcV-1) and Services Functionality Description (SvcV-4).		
2.4.1. Align with IEA Activities	3.3.3.2 – Apply relevant IEA activities to refine, extend, or constrain descriptions of architecture activities and processes so they are consistent with the IEA.	Apply relevant IEA activities to Operational Viewpoints such as the activity models (OV-5 series) and process models (OV-6c).	**Q** - Which IEA activities are relevant to the architecture being developed? **Q** - How do the activities apply to the architecture? **Q** - How are relevant activities applied in the architecture/ program documents?	
2.4.2 Align with IEA Services	3.3.3.4 – Apply relevant IEA services as a basis for defining the services that solutions driven by or resulting from the architecture are	Apply the relevant IEA services to Service Viewpoints descriptions in the architecture being developed. These services may also be described in process models and the Capability to Services Mapping (CV-7).	**Q** – Which IEA services are relevant to the architecture being developed? **Q** – How do the relevant services apply to the architecture? **Q** – How are relevant services addressed in your architecture/	

Compliance Criteria	Appendix D Application Reference	Exemplars for Conveying Compliance	Questions to Address Compliance Criteria	Answers to Questions
	required to deliver.		program documents?	
2.4.3 Align with IEA Rules	3.3.3.3 – Apply relevant IEA rules to operational and service descriptions to ensure resulting capability and service definitions reflect requirements from and are consistent with the description of the IE.	Apply the relevant IEA rules to Operational and Service Viewpoints descriptions especially in activity models (OV-5a), rules models (OV-6a, SvcV-10a), and in process models.	**Q** – Which IEA rules are relevant to the architecture being developed? **Q** – How do the relevant rules apply to the architecture? **Q** – How are relevant rules addressed in your architecture/ program documents?	
2.4.4 Align with IEA Standards	3.3.3.3 – Apply relevant IEA standards to standards descriptions to constrain the implementation and functioning of solutions in ensuring effective operations in the IE.	Apply the relevant IEA standards to Standards and Service Viewpoints descriptions especially in the Standards Profile (StdV-1), Standards Forecast (StdV-2), Services Evolution Description (SvcV-8), and Services Technology & Skills Forecast (SvcV-9) models.	**Q** – Which IEA standards are relevant to the architecture being developed? **Q** – How do the relevant standards apply to the architecture? **Q** – How are relevant standards addressed in your architecture/ program documents?	

Compliance Criteria	Appendix D Application Reference	Exemplars for Conveying Compliance	Questions to Address Compliance Criteria	Answers to Questions
2.5 Align with DoD-wide Reference Architecture (RA)	3.2 RAs provide more detailed descriptions of principles, rules, patterns, and technical positions for key focus areas.	Apply relevant principles, rules, and technical positions from the RA as described earlier in the template. Apply patterns from the RA in process models and other models as appropriate.	**Q** – Which RAs are relevant to the architecture being developed? **Q** – What content in the RAs is relevant to the architecture being developed? **Q** – How does the relevant RA content apply to the architecture? **Q** – How is relevant RA content addressed in the architecture/ program documents?	

Appendix F - Alignment of GIG 2.0 ORA and DoD IEA v1.2 Activities with DoD IEA v2.0 Activities

This appendix contains two tables that map activities from the Global Information Grid (GIG) 2.0 Operational Reference Architecture (ORA) and the DoD Information Enterprise Architecture (IEA) v1.2 to the Department of Defense (DoD) IEA v2.0. This mapping does not indicate a one-for-one replacement of activities in all cases. It is intended to show where relationships between activities exist. In many cases the relationship cannot be understood by the activity name alone, it is understood by reading the definitions. **Table F-1** shows alignment of GIG 2.0 ORA activities with DoD IEA v2.0 activities. **Table F-2** shows alignment of DoD IEA v1.2 activities to DoD IEA v2.0 activities. These tables can be used to assist users who have previously aligned with or used activities from the GIG 2.0 ORA or DoD IEA v1.2, in seeing the mapping of DoD IEA v2.0 activities to previous activities.

Table F-1 – Alignment of GIG 2.0 ORA (v1.5) Activities with DoD IEA v2.0 Activities

GIG 2.0 Activity No.	GIG 2.0 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
A1	Enable Global Authentication, Access Control and Directory Services	A2.1	Enable Global Authentication and Access Control
A1.1	Provide Identity Management and Authentication	A2.1.1	Provide Identity Management and Authentication
A1.1.1	Manage Identity Lifecycle	A2.1.1.1	Manage Identity Lifecycle
A1.1.1.1	Provide Identity Federation	A2.1.3	Provide Federation
A1.1.1.2	Register Identity	A2.1.1.1.1	Register Identity
A1.1.1.3	Maintain Identity	A2.1.1.1.2	Maintain Identity
A1.1.1.4	Expose Identity Information	A2.1.1.1.3	Expose Identity Information
A1.1.2	Provide Credentialing Mechanisms	A2.1.1.2	Provide Credentialing Mechanisms
A1.1.2.1.	Manage Credential	A2.1.1.2.1	Manage Credential
A1.1.2.1.1	Provide Credential Federation	A2.1.3	Provide Federation
A1.1.2.1.2	Issue Credential	A2.1.1.2.1.1	Issue Credential
A1.1.2.1.3	Maintain Credential	A2.1.1.2.1.2	Maintain Credential
A1.1.2.1.4	Expose Credential Information	A2.1.1.2.1.3	Expose Credential Information
A1.1.2.2	Manage Credential Repository	A2.1.1.2.2	Manage Credential Repository
A1.1.3	Authenticate Entity	A2.1.1.3	Authenticate Entity
A1.1.3.1	Provide Authentication Mechanisms	A2.1.1.3.1	Provide Authentication Mechanisms
A1.1.3.2	Validate Credential	A2.1.1.3.2	Validate Credential

GIG 2.0 Activity No.	GIG 2.0 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
	Authenticity		Authenticity
A1.1.3.3	Verify Identity	A2.1.1.3.3	Verify Identity
A1.1.4	Monitor Authentication	A2.1.4	Monitor Authentication and Access Control
A1.1.4.1	Define Authentication Threat	A2.1.4.1	Define Threat Level
A1.1.4.2	Audit Authentication Attempts	A2.1.4.2	Perform Audit
A1.1.4.3	Identify Authentication Threats	A2.1.4.3	Identify Threats
A1.2	Provide Access Control	A2.1.2	Provide Access Control
A1.2.1	Provide Adaptive Access Framework	A2.1.2.1	Provide Adaptive Access Framework
A1.2.1.1	Define Common Attribute Semantics	A2.1.2.1.1	Identify Standard Attributes
A1.2.1.2	Manage Digital Rules	A2.1.5	Manage Digital Rules
A1.2.1.3	Provide Access Controls	A2.1.2.1.2	Enable Access Controls
A1.2.2	Manage Access Process	A2.1.2.2	Manage Access Process
A1.2.2.1	Manage Trust Negotiation	A2.1.2.2.1	Manage Trust Negotiation
A1.2.2.2	Manage Access Privileges	A2.1.2.2.2	Manage Access Privileges
A1.2.3	Monitor Access	A2.1.4	Monitor Authentication and Access Control
A1.2.3.1	Define Access Threat	A2.1.4.1	Define Threat Level
A1.2.3.2	Audit Access	A2.1.4.2	Perform Audit
A1.2.3.3	Identify Access Threat	A2.1.4.3	Identify Threats
A1.3	Provide Directory Services	A3.1.1.3.2	Provide Enterprise Directory Services
A1.3.1	Manage Enterprise Directory	A3.1.1.3.2.1	Manage Enterprise Directory
A1.3.1.1	Provide Directory Federation	A3.1.1.3.2.1.1	Provide Directory Federation
A1.3.1.2	Maintain Entity Attributes	A3.1.1.3.2.1.2	Maintain Entity Attributes
A1.3.2	Publish Enterprise Directory	A3.1.1.3.2.2	Publish Enterprise Directory
A1.3.2.1	Provide Access to Enterprise Directory	A3.1.1.3.2.2.1	Provide Access to Enterprise Directory
A1.3.2.2	Expose Entity Attributes	A3.1.1.3.2.2.2	Expose Entity Attributes
A2	Provide and Use Information and Services from the Edge	A3.1	Provide Information and Services from the Edge
A2.1	Utilize Information, Services, and Applications	A5	Use the IE
A2.1.1	Locate and Use Information, Services, and Applications	A5.1	Locate and Use Information, Services, and Applications
A2.1.1.1	Reactively Discover Information, Services, and Applications	A5.1.1.1	Reactively Discover Information, Services, and Applications
A2.1.1.2	Proactively Discover Information, Services, and Applications	A5.1.1.2	Proactively Discover Information, Services, and Applications

GIG 2.0 Activity No.	GIG 2.0 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
A2.1.1.3	Assess Authenticity	A5.1.2	Establish Authenticity of Discovered Information, Services, or Applications
A2.1.1.4	Assess Utility and Submit Feedback	A5.1.3	Assess Utility of Discovered Information, Services, or Applications
A2.1.2	Share Information	A5.2	Share Information
A2.1.2.1	Post Information	A5.2.1	Post Information
A2.1.2.2	Collaborate	A5.2.2	Collaborate
A2.1.2.2.1	Participate in Real-Time Collaboration	A5.2.2.1	Participate in Real-Time Collaboration
A2.1.2.2.2	Participate in Non-Real-Time Collaboration	A5.2.2.2	Participate in Non-Real-Time Collaboration
A2.2	Provide Information Infrastructure	A3.1.1	Provide Enterprise Services
A2.2.1	Provide Services Infrastructure	A3.1.1.1	Provide Services Infrastructure
A2.2.2	Provide Core Services Infrastructure	A3.1.1.3	Provide Core Services
A2.2.3	Provide Collaboration Infrastructure	A3.1.1.4	Provide Collaboration Services
A2.3	Provide End-User Services & Applications	A3.1.2	Provide End-User Services and Applications
A2.3.1	Provide Mission Oriented Applications	A3.1.2.1	Provide Mission Oriented Applications
A2.3.2	Publish Service	A3.1.2.2	Publish Mission-Oriented Services
A2.4	Ensure Warfighter Trust & Utility	A3.1.3	Enable User Trust and Utility of IE
A2.4.1	Ensure Satisfaction of Information and Services Requirements	A3.1.3.1	Manage Satisfaction of Information and Services Requirements
A2.4.1.1	Ensure Availability	A3.1.3.1.1	Manage Availability
A2.4.1.2	Manage Integrity	A3.1.3.1.2	Manage Integrity
A2.4.1.3	Manage Authenticity	A3.1.3.1.3	Manage Authenticity
A2.4.2	Optimize Information and Services from the Edge	A3.1.3.2	Optimize Information and Services from the Edge
A2.4.2.1	Manage Communities of Interest (COIs)	A3.1.3.2.1	Manage Communities of Interest (COIs)
A2.4.2.2	Provide Common End-User Interfaces	A3.1.3.2.2	Provide Common End-User Interfaces
A2.4.2.3	Ensure Supportability of Multiple User Types	A3.1.3.2.3	Ensure Supportability of Multiple User Types
A3	Provide Joint Infrastructure	A3.2	Provide Joint Infrastructure

GIG 2.0 Activity No.	GIG 2.0 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
A3.1	Provide Computing Infrastructure	A3.2.1	Provide Computing Infrastructure
A3.1.1	Implement Joint Computing Infrastructure	A3.2.1.1	Implement Joint Computing Infrastructure
A3.1.1.1	Acquire Computing Infrastructure Solution	A3.2.1.1.1	Acquire Computing Infrastructure Solution
A3.1.1.2	Install Computing Infrastructure Solution	A3.2.1.1.2	Install Computing Infrastructure Solution
A3.1.1.3	Integrate Computing Infrastructure Solution	A3.2.1.1.3	Integrate Computing Infrastructure Solution
A3.1.1.4	Install Computing Infrastructure Solution	A3.2.1.1.4	Deploy Computing Infrastructure Solution
A3.1.1.5	Test Computing Infrastructure Solution	A3.2.1.1.5	Test and Accredit Computing Infrastructure Solution
A3.1.2	Provide Computing Infrastructure Net-Centric Environment	A3.2.1.2	Establish Computing Infrastructure Environment
A3.1.2.1	Provide Self-Managing Computing Infrastructure Operations	A3.2.1.2.1	Provide Self-Managing Computing Infrastructure Operations
A3.1.2.2	Provide Hardware Environment	A3.2.1.2.2	Provide Hardware Environment
A3.1.2.3	Provide Storage Environment	A3.2.1.2.3	Provide Storage Environment
A3.1.2.4	Provide Software Environment	A3.2.1.2.4	Provide System Software Environment
A3.1.2.5	Provide High Productivity Computing Infrastructure Environment	A3.2.1.2.5	Provide High Productivity Computing Environment
A3.1.2.6	Provide Grid Computing Infrastructure	A3.2.1.2.6	Provide Grid Computing Environment
A3.1.2.7	Provide Computing Infrastructure Services	A3.2.1.2.7	Provide Computing Infrastructure Services
A3.1.2.8	Provide COCOM Aligned Service Centers	A3.2.1.2.8	Provide COCOM Aligned Service Centers
A3.2	Provide Communications Infrastructure	A3.2.2	Provide Communications Infrastructure
A3.2.1	Ensure Interoperability of GIG Components	A3.2.2.1	Procure Interoperable Transport Components
A3.2.1.1	Standardize Extensions to Other Network Infrastructures	A3.2.2.2	Standardize Extensions to Other Network Infrastructures
A3.2.1.2	Support Technology Insertion, Reuse, and Retirement	A3.3.2	Evolve Communications Infrastructure
A3.2.2	Provide Global Connectivity to	A3.2.2.3	Provide Global Connectivity

GIG 2.0 Activity No.	GIG 2.0 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
	Support the Warfighter		
A3.2.2.1	Provide WAN Connectivity	A3.2.2.3.1	Provide Wide Area Network (WAN) Connectivity
A3.2.2.2	Provide LAN Connectivity	A3.2.2.3.2	Provide Local Area Network (LAN) Connectivity
A3.2.2.3	Provide Ad-hoc Connectivity	A3.2.2.3.3	Provide Ad Hoc Connectivity
A3.2.3	Provide Communications Support Mechanisms	A3.2.2.4	Provide Communication Support Mechanisms
A3.2.3.1	Provide QoS Mechanisms	A3.2.2.4.1	Provide Quality of Service (QoS) Mechanisms
A3.2.3.2	Provide Security Mechanisms	A3.2.2.4.2	Enable Security Mechanisms
A4	Implement Common Policies and Standards	A1.1	Provide Common Policies and Standards
A4.1	Develop GIG Overarching Requirements	A1.1.1	Develop IE Vision and Strategy
A4.1.1	Develop GIG Interoperability Policy	A1.1.1.1	Define IE Interoperability
A4.1.2	Develop GIG Common Architecture Policy	A1.1.1.2	Determine Common Infrastructure Architecture Requirements
A4.1.3	Develop GIG Audit Requirements Policy	A1.1.1.3	Enable IE Audit
A4.1.4	Develop GIG Evolution Strategy	A1.1.1.4	Develop IE Evolution Strategy
A4.1.5	Develop and Enforce Joint/ Enterprise Level Governance	A1.2	Implement Joint/Enterprise Level Governance of the IE
A4.1.6	Support Precedence Policies	A1.1.1.5	Develop Precedence-Based Services Strategy
A4.1.7	Develop GIG Acquisitions Strategy	A1.1.1.6	Develop IE Acquisition Strategy
A4.1.8	Develop Joint Training Strategy	A1.1.1.7	Develop Joint Training Strategy
A4.2	Develop Functional Policy	A1.1.2	Develop IE Functional Policy
A4.2.1	Develop NetOps Policy	A1.1.2.1	Develop NetOps Policy
A4.2.2	Develop NetOps C2 Policy	A1.1.2.2	Develop NetOps Command and Control (C2) Policy
A4.2.3	Develop Quality of Service (QoS) Policy	A1.1.2.3	Develop Quality of Service (QoS) Policy
A4.2.4	Develop Quality of Protection (QoP) Policy	A1.1.2.4	Develop Quality of Protection (QoP) Policy
A4.2.5	Develop Communications Policy	A1.1.2.5	Develop Communications Policy
A4.2.6	Develop Joint Spectrum Assignment Plan	A1.1.2.6	Develop Joint Spectrum Assignment Plan

GIG 2.0 Activity No.	GIG 2.0 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
A4.2.7	Develop Information Sharing Policy	A1.1.2.7	Develop Information Sharing Policy
A4.2.8	Develop Configuration Management Policy	A1.1.2.8	Develop Configuration Management Policy
A4.2.9	Develop IA Policy	A1.1.2.9	Develop IA Policy
A4.2.9.1	Develop C&A Policy	A1.1.2.9.1	Develop IA Certification & Accreditation (C&A) Policy
A4.2.9.2	Develop IdM & Authentication Policy	A1.1.2.9.2	Develop Identity Management and Authentication (IdM&A) Policy
A4.2.9.3	Develop Access Control Policy	A1.1.2.9.3	Develop Access Control Policy
A4.3	Enforce Common Development Standards	A1.1.3	Establish IE Standards
A4.3.1	Define and Develop NetOps Standards	A1.1.3.1	Develop NetOps Standards
A4.3.2	Define and Develop IA Standards	A1.1.3.2	Develop IA Standards
A4.3.3	Define and Develop Communications Standards	A1.1.3.3	Develop Communications Standards
A4.3.4	Define and Develop Computing Infrastructure Standards	A1.1.3.4	Develop Computing Infrastructure Standards
A4.3.5	Define and Develop Data/ Service Standards	A1.1.3.5	Develop Data/Service Standards
A5	Enforce Unity of Command	A4	Control and Operate the IE
A5.1	Enable Commander’s NetOps Intent	A4.1	Establish Commander's Intent for NetOps
A5.1.1	Develop Commander’s Intent for GIG NetOps	A4.1.1	Develop Commander's Intent for NetOps
A5.1.2	Promulgate Commander’s Intent for GIG NetOps	A4.1.2	Communicate Commander's Intent for NetOps
A5.1.3	Monitor Commander’s Intent for GIG NetOps	A4.1.3	Monitor Accomplishment of Commander's Intent for NetOps
A5.2	Enable GIG C2 Through NetOps	A4.2	Exercise Operational Control of IE Through NetOps
A5.2.1	Manage GIG Situational Awareness	A4.2.1	Manage IE Situational Awareness
A5.2.1.1	Produce GIG Situational Awareness Data	A4.2.1.1	Produce IE Situational Awareness Information
A5.2.1.2	Collect GIG Situational Awareness Data	A4.2.1.2	Collect IE Situational Awareness Data
A5.2.1.3	Report on GIG Situational	A4.2.1.3	Report IE Situational

GIG 2.0 Activity No.	GIG 2.0 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
	Awareness		Awareness
A5.2.1.4	Respond to GIG Situation	A4.2.2	Respond to IE Situation
A5.2.2	Provide GIG Enterprise Management (GEM)	A4.2.3	Conduct Enterprise Management of IE
A5.2.2.1	Manage GIG Resource Allocation	A4.2.3.1	Allocate IE Resources
A5.2.2.2	Perform System Administration	A4.2.3.2	Perform System Administration
A5.2.2.3	Provide Change Management	A4.2.3.3	Provide Change Management
A5.2.2.4	Provide Configuration Control	A4.2.3.4	Provide Configuration Control
A5.2.2.5	Perform Tech Refresh	A4.2.3.5	Perform Tech Refresh
A5.2.2.6	Perform Patch Management	A4.2.3.6	Perform Patch Management
A5.2.2.7	Provide Performance Management	A4.2.3.7	Manage IE Performance
A5.2.2.8	Provide Joint Spectrum Management	A4.2.3.1.1.5	Allocate Electromagnetic Spectrum
A5.2.2.9	Provide Satellite Communications Management	A4.2.3.1.1.6	Manage Satellite Communications (SATCOM)
A5.2.3	Conduct GIG Network Defense (GND)	A4.2.4	Conduct Network Defense
A5.2.3.1	Provide Secure Transfer Services	A2.2	Enable Cross Domain Security
A5.2.3.2	Provide Enclave, Network and Boundary Protection	A2.3.1	Protect Network and Enclave Boundaries
A5.2.3.3	Provide Network Resource Management Mechanism Protection	A2.3.2	Manage Network Resources to Defend IE
A5.2.3.4	Provide IT Platform Protection	A2.3.3	Provide IT Platform Protection
A5.2.3.5	Provide Data Protection	A2.3.4	Enable Data Protection
A5.2.3.6	Provide Security Monitoring, Vulnerability Analysis, and Threat Identification	A4.2.4.1	Provide Security Monitoring, Vulnerability Analysis, and Threat Identification
A5.2.3.7	Perform Threat/Incident Management	A4.2.4.2	Perform Threat/Incident Management
A5.2.3.8	Provide Critical Infrastructure Protection (CIP)	A4.2.4.3	Provide Critical Infrastructure Protection (CIP)
A5.2.4	Conduct GIG Content Management	A4.2.5	Perform Content Management
A5.2.4.1	Prioritize Information Resources	A4.2.5.1	Prioritize Information Resources
A5.2.4.2	Monitor Information Delivery	A4.2.5.3	Monitor Information

GIG 2.0 Activity No.	GIG 2.0 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
			Delivery
A5.3	Manage Operational Risk	A2.3.5	Manage IAVA Compliance
A5.3.1	Oversee Certification and Accreditation Program	A2.4	Manage IE Certification and Accreditation (C&A) Program
A5.3.2	Manage IAVA Compliance	A2.3.5	Manage IAVA Compliance
A5.3.3	Issue Task Orders	A4.2.4.4	Issue IAVA) Task Orders
A5.4	Provide Common Training Readiness	A5.3	Maintain IE Proficiency
A5.4.1	Identify Mission Capability Requirements	A5.3.1	Identify Mission Capability Requirements for IE Proficiency
A5.4.2	Develop Common Training Plan	A5.3.2	Develop Common Training Plan for IE Proficiency
A5.4.3	Execute Common Training Plan	A5.3.3	Execute Common Training Plan for IE Proficiency
A5.4.4	Assess Training Performance	A5.3.4	Assess Training Performance

Table F-2 – Alignment of DoD IEA v1.2 Activities with DoD IEA v2.0 Activities

DoD IEA v1.2 Activity No.	DoD IEA v1.2 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
A1	Provide Data and Services Deployment	A3.1	Provide Information and Services from the Edge
A11	Provide Discovery Services	A3.1.1.3.3	Provide Discovery Services
A111	Provide Data, Service and IT Resource Registration Services	A3.1.1.3.3.1	Provide Registration Services
A112	Provide Data, Service and IT Resource Search Services	A3.1.1.3.3.2	Provide Search Services
A12	Provide Core Enterprise Services	A3.1.1.3	Provide Core Services
A121	Provide SOA Foundational Services	A3.1.1.3.1	Provide Service Oriented Architecture Foundation (SOAF) Services
A122	Promote Data and Service Separation from Applications	A3.1.1.2	Enable Data and Service Separation from Applications
A13	Provide Collaboration Services	A3.1.1.4	Provide Collaboration Services
A131	Provide Other Collaboration Services	A3.1.1.4.1	Provide Other Collaboration Services
A132	Provide Messaging Service	A3.1.1.4.2	Provide Messaging Services
A133	Provide Awareness Services	A3.1.1.4.3	Provide Awareness Services
A14	Provide Common End-User Interfaces	A3.1.3.2.2	Provide Common End-User Interfaces
A141	Provide Data in a Manner That Meets End-User Needs	A3.1.3.2.2.1	Provide Data to Meet End-User Needs
A142	Provide Flexible and Agile Services	A3.1.3.2.2.2	Provide Flexible and Agile Services
A15	Develop Design Patterns for Data & Services	A1.1.3.5	Develop Data/Service Standards
A151	Ensure Services Follow Net-Centric Services Strategy	A1.1.3.5.1	Enforce Net-Centric Services Strategy as a Standard
A152	Ensure Data Follows Net Centric Data Strategy	A1.1.3.5.2	Enforce Net-Centric Data Strategy as a Standard
A153	Migrate Technologies to Standards	A1.1.3.5.3	Migrate Technologies to Standards
A16	Foster Development for Standard Semantics	A1.1.3.7	Develop and Enforce Common Semantics
A161	Coordinate Metadata for	A1.1.3.6	Develop Metadata Standards

DoD IEA v1.2 Activity No.	DoD IEA v1.2 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
	Data, Services, and IT Resources		
A162	Coordinate Communities of Interest (COIs)	A3.1.3.2.1	Manage Communities of Interest (COIs)
A17	Enable Trust	A3.1.3	Enable User Trust and Utility of IE
A171	Manage Integrity	A3.1.3.1.2	Manage Integrity
A172	Manage Pedigree	A3.1.3.1.3	Manage Authenticity
A2	Provide Secured Availability	A2	Protect and Secure the IE
A21	Provide Secure Transfer Services (CDS)	A2.2	Enable Cross Domain Security
A211	Issue and Administer Information Discovery Initiatives	A2.2.1	Enable Cross Domain Information Discovery
A212	Issue and Administer Information Transfer Initiatives	A2.2.2	Enable Cross Domain Information Exchange and Service Invocation
A2121	Oversee CDS Initiatives	A2.2.3	Manage CDS Initiatives
A21211	Manage Data Type Definitions	A2.2.3.1	Participate in Unified Cross Domain Management Office (UCDMO)
A21212	Oversee E2E Solution Implementation	A2.2.3.2	Deliver Cross Domain Solutions as Enterprise Services
A2122	Oversee DoD Migration from P2P to E2E Accreditation	A2.2.4	Implement End-to-End Security Accreditation
A22	Provide Enclave, Network and Boundary Protection	A2.3.1	Protect Network and Enclave Boundaries
A221	Provide Technical Protection Standards	A2.3.1.1	Provide Technical Protection Standards
A222	Provide Protective Architectures	A2.3.1.2	Issue Enclave Protection Policy
A23	Provide Network Resource Management Mechanism Protection	A2.3.2	Manage Network Resources to Defend IE
A24	Provide C&A Services	A2.4	Manage IE Certification and Accreditation (C&A) Program
A241	Govern GIG-wide C&A	A2.4.1	Govern Enterprise-wide C&A
A2411	Manage/Provide Automated C&A Services	A2.4.2	Provide Automated C&A Services
A242	Oversee Development of	A1.1.2.9.1	Develop IA Certification &

DoD IEA v1.2 Activity No.	DoD IEA v1.2 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
	Unified C&A Standards and Processes		Accreditation (C&A) Policy
A2421	Oversee Development of a DoD C&A Migration Strategy	A1.1.2.9.1	Develop IA Certification & Accreditation (C&A) Policy
A25	Provide IA Workforce	A2.5	Provide IA Workforce
A251	Oversee Identification of IA Positions	A2.5.1	Identify DoD IA Positions
A252	Oversee Identification, Tracking, and Management of IA Personnel	A2.5.2	Manage IA Personnel Lifecycle
A253	Oversee DoD IA Training and Education	A2.5.3	Oversee DoD IA Training and Education
A254	Promote GIG User Awareness	A2.5.4	Implement IA Orientation and Awareness
A255	Provide IA Tools and Services	A2.5.3	Oversee DoD IA Training and Education
A26	Provide IT Platform Protection	A2.3.3	Provide IT Platform Protection
A261	Manage/Provide Integrated Assessment Process	A2.3.3.1	Assess Vulnerability of Potential IT Platforms
A262	Participate in Developing National E/P Acquisition Standards	A2.3.3.2	Support National Vulnerability Evaluation and Acquisition Requirements Development
A27	Provide Assured Control of the GIG	A2.6	Provide Assured Control of IE
A271	Manage CND & IA Services	A2.6.1	Manage Computer Network Defense (CND) and IA Services
A272	Provide Configuration and Policy Based Management	A2.6.2	Provide Policy-Based Management of IA Components of IE
A2721	Manage Technology and Infrastructure	A2.6.2.1	Manage Technology and Infrastructure for IA Policy Management
A2722	Provide Policy Architecture	A2.6.2.2	Implement Architecture for IA Policy Management
A2723	Oversee Operational Management Process	A2.6.2.3	Provide Operational Management of IA
A28	Provide Identity, Authentication, and Privilege Management	A2.1	Enable Global Authentication and Access Control
A281	Develop Adaptive Access	A2.1.2.1	Provide Adaptive Access

DoD IEA v1.2 Activity No.	DoD IEA v1.2 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
	Framework		Framework
A282	Manage IA & PM Policy Evolution	A1.1.2.9.2	Develop Identity Management and Authentication (IdM&A) Policy
A283	Oversee Identity Management Initiatives	A2.1.1	Provide Identity Management and Authentication
A2831	Managing Identity Lifecycles	A2.1.1.1	Manage Identity Lifecycles
A2832	Manage Credentialing Process	A2.1.1.2.1	Manage Credential
A284	Oversee Authentication Initiatives	A2.1.1	Provide Identity Management and Authentication
A2841	Manage Authentication Processes	A2.1.1.3	Authenticate Entity
A285	Oversee Privilege Management Processes	A2.1.2.2.2	Manage Access Privileges
A2851	Manage Subject Attribute Model Development	A2.1.2.1.1	Identify Standard Attributes
A28511	Manage Privilege Lifecycle Development	A2.1.2.2.2	Manage Access Privileges
A2852	Manage Attribute Repository	A3.1.1.3.2.1.2	Maintain Entity Attributes
A29	Provide EIMS	A2.7	Tag Data Objects with IA Metadata
A291	Oversee IA Crypto Binding Tool Initiative	A2.7.1	Bind IA Metadata Tags to Data Objects
A292	Oversee IA Metadata Tag Initiative	A2.7.2	Develop IA Metadata Tagging Standards
A2(10)	Provide Data-in-Transit and Data-at-Rest Protection	A2.3.4	Enable Data Protection
A2(10)1	Provide Data-at-Rest Protection	A2.3.4.1	Standardize Data-at-Rest Protection
A2(10)2	Oversee Development of an Evolution Strategy	A2.3.4.2	Standardize Data-in-Transit Protection
A2(10)21	Manage IPv6 Migration Strategy	A2.3.4.2.1	Manage Security Strategy for Data-in-Transit over IPv6
A2(10)22	Manage NIPRNet / Internet Integration Initiatives	A2.3.4.2.2	Protect Data-in-Transit Between NIPRNet and Internet
A2(10)23	Manage System High-System Integration Initiatives	A2.3.4.2.3	Protect Data-in-Transit Across System High Boundaries

DoD IEA v1.2 Activity No.	DoD IEA v1.2 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
A2(10)24	Manage Component Architecture Integration Initiatives	A2.3.4.2.4	Integrate Data-in-Transit Protection Across Architecture Components
A2(10)25	Manage Coalition Sharing Initiatives	A2.3.4.2.5	Protect Data-in-Transit during Coalition Information Sharing
A2(11)	Provide for Federation	A2.1.3	Provide Federation
A2(11)1	Manage DoD's Participation in Federation	A2.1.3.1	Manage DoD's Participation in Federation
A2(11)11	Manage Federation Rules	A2.1.3.3	Manage Federation Rules
A2(11)2	Synchronize and Deconflict DoD IA Attributes	A2.1.3.2	Synchronize and Deconflict DoD IA Attributes
A2(12)	Manage Mission Assurance Processes	A2.8	Manage Mission Assurance
A2(12)1	Provide Software Assurance Process	A2.8.1	Evaluate Software Assurance
A2(12)2	Provide Hardware Assurance Process	A2.8.2	Evaluate Hardware Assurance
A2(12)3	Provide System Assurance Process	A2.8.3	Evaluate System Assurance
A2(12)4	Provide Supplier Assurance Process	A2.8.4	Evaluate Supplier Assurance
A2(13)	Provide for Globalization	A2.9	Manage Globalization Risks
A3	Provide Computing Infrastructure Readiness	A3.2.1	Provide Computing Infrastructure
A31	Develop and Implement Computing Infrastructure	A3.2.1.1	Implement Joint Computing Infrastructure
A311	Develop / Enforce Computing Standards	A1.1.3.4	Develop Computing Infrastructure Standards
A312	Acquire Computing Infrastructure Solution(s)	A3.2.1.1.1	Acquire Computing Infrastructure Solution
A313	Install Computing Infrastructure Solution(s)	A3.2.1.1.2	Install Computing Infrastructure Solution
A314	Integrate Computing Infrastructure Solution(s)	A3.2.1.1.3	Integrate Computing Infrastructure Solution
A315	Deploy Computing Infrastructure Solution(s)	A3.2.1.1.4	Deploy Computing Infrastructure Solution
A316	Test and Accredit Computing Infrastructure Solution(s)	A3.2.1.1.5	Test and Accredit Computing Infrastructure Solution
A32	Provide Computing Infrastructure Net-Centric Environments	A3.2.1.2	Establish Computing Infrastructure Environment

DoD IEA v1.2 Activity No.	DoD IEA v1.2 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
A321	Provide Self Managing CI Operations	A3.2.1.2.1	Provide Self-Managing Computing Infrastructure Operations
A3211	Automate Computing Infrastructure Operations	A3.2.1.2.1.1	Automate Computing Infrastructure Operations
A3212	Support Data Fusion	A3.2.1.2.1.2	Enable Automated NetOps Information Reporting in Computing Infrastructure
A3213	Enable Dynamic GIG Processing Utilization	A3.2.1.2.1.3	Enable Dynamic, Virtual Processing in Computing Infrastructure
A322	Provide Hardware Environment	A3.2.1.2.2	Provide Hardware Environment
A323	Provide Storage Environment	A3.2.1.2.3	Provide Storage Environment
A324	Provide Software Environment	A3.2.1.2.4	Provide System Software Environment
A325	Provide High Productivity Computing Infrastructure Environment	A3.2.1.2.5	Provide High Productivity Computing Environment
A326	Provide Autonomous Environment	A3.2.1.2.1.4	Provide Autonomous CI Environment
A327	Provide Grid Computing Infrastructure Environment	A3.2.1.2.6	Provide Grid Computing Environment
A328	Provide Computing Infrastructure Services	A3.2.1.2.7	Provide Computing Infrastructure Services
A3281	Provide Shared Computing	A3.2.1.2.7.1	Provide Shared Computing
A3282	Provide Computing Infrastructure Storage Services	A3.2.1.2.7.2	Provide Computing Infrastructure Storage Services
A3283	Provide Operating System (OS) Services	A3.2.1.2.7.3	Provide Operating System (OS) Services
A32831	Provide Runtime Services	A3.2.1.2.7.4	Provide Runtime Services
A3284	Provide Operation Oversight Services	A3.2.1.2.7.5	Provide Operation Oversight Services
A3285	Assess Computing Infrastructure Related User Needs	A3.2.1.2.7.6	Assess Computing Infrastructure Requirements and Performance
A329	Provide Application Migration Support	A3.2.1.2.7.7	Provide Application Migration Support
A32(10)	Perform Computing Infrastructure IA Support	A3.2.1.2.9	Provide IA for Computing Infrastructure

DoD IEA v1.2 Activity No.	DoD IEA v1.2 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
A32(10)1	Perform CI IA Encryptions for Shared Storage and Media Functions	A3.2.1.2.9.1	Enable IA for Shared Storage and Media Functions
A32(10)2	Ensure Secure Interoperability	A3.2.1.2.9.2	Enable Secure Interoperability
A32(10)3	Provide Trusted Computing	A3.2.1.2.9.3	Provide Trusted Computing
A33	Provide Computing Infrastructure Controls	A3.2.1.3	Provide Computing Infrastructure Controls
A331	Provide Security Control Mechanisms	A3.2.1.3.1	Provide Security Control Mechanisms for CI
A3311	Provide Access Controls	A2.1.2.1.2	Enable Access Controls
A3312	Provide Privilege Controls	A3.2.1.3.1.1	Provide Privilege Controls for CI Resources
A3313	Provide Hardware and Operating System Security Configuration Controls	A3.2.1.3.1.2	Provide Hardware and Operating System Security Configuration Controls
A332	Perform Computing Infrastructure Configuration Management	A4.2.3.4	Provide Configuration Control
A333	Performance Management	A4.2.3.7	Manage IE Performance
A3331	Develop and Apply CI Metrics for Testing and Development	A4.2.3.7.1	Develop and Apply IE Performance Metrics
A3332	Conduct Computing Infrastructure Performance Assessment	A4.2.3.7.2	Assess Performance of IE Resources
A3333	Provide Optimization / Performance Controls	A3.2.1.3.2	Provide Optimization / Performance Controls
A3334	Parameterize GIG Resources	A3.2.1.3.3	Parameterize CI Resources
A334	Maintain Computing Infrastructure	A3.2.1.4	Maintain Computing Infrastructure
A34	Allocate Computing Infrastructure Resources	A4.2.3.1.2	Allocate Computing Infrastructure Resources
A341	Allocate Computing Resources	A4.2.3.1.2.1	Allocate Computing Resources
A3411	Allocate Shared Computing Resources	A4.2.3.1.2.1.1	Allocate Shared Computing Resources
A3412	Allocate Processing	A4.2.3.1.2.1.2	Allocate Processing Resources
A3413	Allocate Operations Across Hardware Resources	A4.2.3.1.2.1.3	Allocate Operations Across Hardware Resources
A342	Allocate Storage Resources	A4.2.3.1.2.2	Allocate Storage Resources
A343	Allocate Network Interfaces	A4.2.3.1.2.3	Allocate Network Interfaces
A344	Allocate Physical Facilities	A4.2.3.1.2.4	Allocate Physical Facilities

DoD IEA v1.2 Activity No.	DoD IEA v1.2 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
A35	Facilitate Computing Infrastructure Knowledge Management	A3.2.1.5	Provide Information on Computing Infrastructure Resources
A351	Provide Computing Infrastructure Metadata	A3.2.1.5.1	Provide Computing Infrastructure Metadata
A3511	Develop Computing Infrastructure Ontology	A3.2.1.5.1.1	Develop Computing Infrastructure Ontology
A3512	Ensure Computing Infrastructure Metadata is Discoverable	A3.2.1.5.1.2	Register Computing Infrastructure Metadata
A3513	Provide Computing Infrastructure Functionality Information	A3.2.1.5.1.3	Provide Computing Infrastructure Functionality Information
A3514	Provide Computing Infrastructure Capacity Information	A3.2.1.5.1.4	Provide Computing Infrastructure Capacity Information
A3515	Provide Computing Infrastructure Asset Location Information	A3.2.1.5.1.5	Provide Computing Infrastructure Asset Location Information
A352	Provide Computing Infrastructure Support to NetOps	A3.2.1.5.2	Provide Computing Infrastructure Availability and Access Information
A3521	Provide Computing Infrastructure Availability Information	A3.2.1.5.2.1	Provide Computing Infrastructure Availability Information
A3522	Provide Computing Infrastructure Access Information	A3.2.1.5.2.2	Provide Computing Infrastructure Access Information
A36	Evolve Computing Infrastructure	A3.3.1	Evolve Computing Infrastructure
A361	Advance Computing Infrastructure Technology	A3.3.1.1	Enhance Computing Infrastructure with New Technology
A3611	Perform Technology Forecast	A3.3.1.1.1	Develop Technology Forecast
A3612	Conduct Research and Development Efforts	A3.3.1.1.2	Conduct Research and Development
A3613	Determine Implication of Technology Development for DoD Mission	A3.3.1.1.3	Assess Changes to Computing Infrastructure
A362	Accomplish Computing Infrastructure Transition Planning	A3.3.1.2	Develop Transition Plans for Computing Infrastructure

DoD IEA v1.2 Activity No.	DoD IEA v1.2 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
A4	Provide Communications Readiness	A3.2.2	Provide Communications Infrastructure
A41	Support Interoperability of All GIG Components	A3.2.2.1	Procure Interoperable Transport Components
A411	Support Interoperability Standards	A1.1.3.3	Develop Communications Standards
A412	Support Technology Insertion, Reuse and Retirement	A3.3.2	Evolve Communications Infrastructure
A413	Allocate Electromagnetic Spectrum	A4.2.3.1.1.5	Allocate Electromagnetic Spectrum
A4131	Optimize Spectrum Use	A4.2.3.1.1.5.1	Optimize Spectrum Use
A4132	Support Compatibility with Other Systems (e.g. Non-GIG Systems)	A4.2.3.1.1.5.2	Enable RF Communications with Mission Partners
A42	Provide Physical Connectivity	A3.2.2.3	Provide Global Connectivity
A421	Support Enterprise Users	A3.2.2.3.1	Provide Wide Area Network (WAN) Connectivity
A422	Support Regional Users	A3.2.2.3.2	Provide Local Area Network (LAN) Connectivity
A423	Support Deployed Users	A3.2.2.3.3	Provide Ad Hoc Connectivity
A43	Support QoS Standards	A3.2.2.4.1	Provide Quality of Service (QoS) Mechanisms
A431	Support Service Level Agreements	A3.2.2.4.1.1	Support Service Level Agreements
A432	Facilitate Continuity of Service	A3.2.2.4.1.2	Facilitate Continuity of Communications Service
A4321	Support Reliability / Maintainability / Availability Standards	A3.2.2.4.1.2.1	Implement Reliability, Maintainability, and Availability (RMA) Standards
A4322	Support System Redundancy	A3.2.2.4.1.2.2	Enable System Redundancy
A433	Support Precedence Policies	A3.2.2.4.1.3	Follow Precedence Policies
A44	Plan Resource Allocation	A4.2.3.1.1.1	Plan Communications Resource Allocation
A441	Support Surge Loading	A4.2.3.1.1.2	Support Surge Loading
A442	Support Multiple Military Operations	A4.2.3.1.1.3	Support Multiple Military Operations
A443	Support Day-to-Day Operations	A4.2.3.1.1.4	Support Day-to-Day Operations
A5	Provide NetOps Agility	A4	Control and Operate the IE
A51	Expose GIG Situational Awareness Info	A4.2.1.3	Report IE Situational Awareness

DoD IEA v1.2 Activity No.	DoD IEA v1.2 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
A511	Publish GIG Situational Awareness Info	A4.2.1.3.1	Publish IE Situational Awareness Information
A512	Subscribe GIG Situational Awareness Info	A4.2.1.3.2	Subscribe to IE Situational Awareness Information
A513	Advertise GIG Situational Awareness Info	A4.2.1.3.3	Advertise IE Situational Awareness Information
A52	Facilitate Assured Access to GIG Situational Awareness Information	A4.2.1.3.4	Facilitate Assured Access to IE Situational Awareness Information
A521	Manage Access Control	A4.2.1.3.4.1	Manage Access to IE Situational Awareness Information
A522	Create / Maintain Shared Space	A4.2.1.3.4.2	Create/Maintain Shared Space for IE Situational Awareness Information
A53	Manage Information Exchange Resources	A4.2.5	Perform Content Management
A531	Prioritize Information Infrastructure Demands	A4.2.5.1	Prioritize Information Resources
A532	Optimize Information Infrastructure Use	A4.2.5.2	Optimize Information Infrastructure Use
A54	Produce Relevant GIG Situational Awareness	A4.2.1.1	Produce IE Situational Awareness Information
A541	Process GIG Situation Awareness Information	A4.2.1.1.1	Process IE Situational Awareness Data
A542	Generate GIG Situational Awareness Information	A4.2.1.2	Collect Situational Awareness Data
A543	Create Tailorable Visualizations	A4.2.1.1.2	Create Tailorable Visualizations
A55	Perform Operational Control	A4.2	Exercise Operational Control of IE Through NetOps
A551	Perform GIG Enterprise Management (GEM)	A4.2.3	Conduct Enterprise Management of IE
A552	Perform GIG Network Defense	A4.2.4	Conduct Network Defense
A553	Perform GIG Content Management	A4.2.5	Perform Content Management
A554	Develop Response to the GIG Situation	A4.2.2.1	Develop Response to IE Situation
A555	Select Response to the GIG Situation	A4.2.2.2	Select Response to IE Situation
A556	Coordinate Response to the GIG Situation	A4.2.2.3	Coordinate Response to IE Situation

DoD IEA v1.2 Activity No.	DoD IEA v1.2 Activity Name	DoD IEA v2.0 Activity No.	DoD IEA v2.0 Activity Name
A557	Execute Response to the GIG Situation	A4.2.2.4	Execute Response to IE Situation
A56	Measure Effectiveness of GIG	A4.2.3.8	Measure IE Effectiveness
A561	Measure Operational GIG Effectiveness	A4.2.3.8.1	Measure Operational Effectiveness of NetOps
A562	Measure Strategic GIG Effectiveness	A4.2.3.8.2	Measure Strategic Effectiveness of IE
A57	Manage Operational Policy	A1.1.2.1	Develop NetOps Policy
A571	Administer NetOps Policies	A1.1.2.1.1	Administer NetOps Policy
A572	Monitor NetOps Policies	A1.1.2.1.2	Monitor NetOps Policy
A573	Enforce NetOps Policies	A1.1.2.1.3	Enforce NetOps Policy
A58	Establish Commander's NetOps Intent	A4.1	Establish Commander's Intent for NetOps
A581	Develop Commander's Intent for GIG NetOps	A4.1.1	Develop Commander's Intent for NetOps
A582	Promulgate Commander's Intent for GIG NetOps	A4.1.2	Communicate Commander's Intent for NetOps
A583	Monitor Commander's Intent for GIG NetOps	A4.1.3	Monitor Accomplishment of Commander's Intent for NetOps
A59	Plan GIG NetOps	A4.3	Plan IE NetOps
A591	Determine Requirements	A4.3.1	Determine NetOps Requirements
A592	Develop Plans	A4.3.2	Develop NetOps Plans
A593	Coordinate Plans	A4.3.3	Coordinate NetOps Plans
A594	Implement NetOps Plans	A4.3.4	Implement NetOps Plans
A5(10)	Evolve NetOps Capabilities	A3.3.3	Evolve Network Operations (NetOps) Capabilities

Appendix G: DoD Enterprise Architecture (EA) Compliance Requirements

1. Introduction/Purpose

This appendix describes what each program or initiative implementing a system, service, or solution that interacts with or is part of the Information Enterprise (IE) must do to comply with the Department of Defense (DoD) Enterprise Architecture (EA)[19]. For the purposes of this appendix, compliance includes conformance, alignment, and adherence as prescribed in this appendix. The DoDD 8000.01, *Management of the Department of Defense Information Enterprise*, February 10, 2009 describes the DoD EA as: "A federation of descriptions that provide context and rules for accomplishing the mission of the Department. These descriptions are developed and maintained at the Department, Capability, and Component levels and collectively define the people, processes, and technology required in the "current" and "target" environments; and the roadmap for transition to the target environment." The framework for the DoD EA, shown in **Figure 1**, provides the conceptual structure for the DoD EA. This framework provides the basis for describing, developing, relating, and using the multitude of artifacts that comprise the DoD EA.

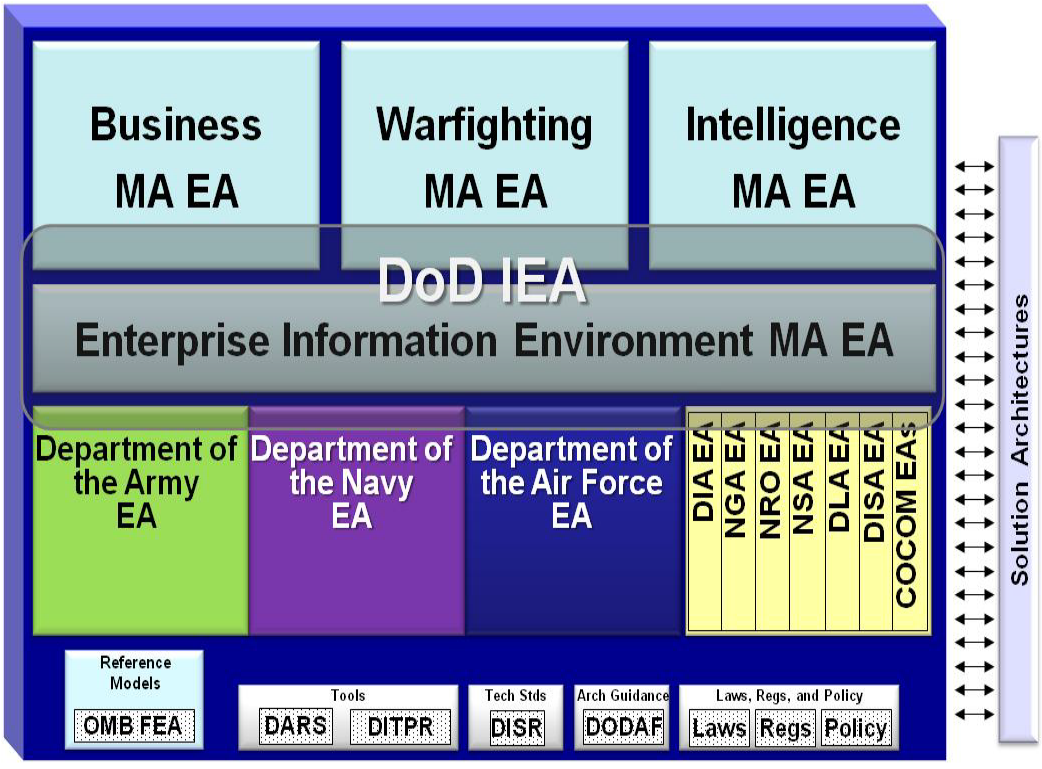


Figure 1- DoD Enterprise Architecture Framework

[19] The content in this appendix describing the compliance requirements for the EA is expected to eventually find its way into appropriate EA Policy and guidance. It is provided here in the DoD IEA to establish the guidance and a means to enforce the guidance until it is captured in appropriate EA Policy and guidance.

The components of the DoD EA include strategic guidance such as policy; the DoD Architecture Framework (DoDAF); the OMB FEA reference models; tools such as repositories and registries; and the set of federated Command/Service/Agency (C/S/A) enterprise, reference, and solution architectures. Collectively, these elements comprise the principles, rules, patterns, activities, services, standards, and core enterprise capabilities around which all DoD solutions are built. The OMB FEA is shown as part of the DoD EA because the reference models and taxonomies of the FEA guide and constrain the reference models, taxonomies and architectures of the DoD EA.

The primary purpose of the DoD EA is to provide a common and coherent means to guide investment portfolio strategies and decisions, define capability and interoperability requirements, provide DoD applicable standards, represent security and information assurance requirements, and provide a sound basis for transitioning from the existing environment to the future. To achieve this, all DoD system, services and solutions that interact with or are part of the IE are required to comply and align with appropriate portions of the DoD EA. Compliance with the DoD EA is a responsibility distributed across DoD and is required by program managers and decision-makers at every stage of designing, developing, and executing a solution.

2. DoD EA Compliance Requirements

Compliance with the DoD EA is necessary to ensure a unified approach across the Department in achieving the goals and objectives of the IE. Compliance requirements for the DoD EA focus on the descriptive content of key artifacts and the relationships established in the federation of the DoD EA. Compliance criteria explicitly describes the specific content that must be applied and is typically relegated to architecture development. It can also apply to physical solutions, especially with respect to compliance with technical direction. Other forms of compliance, such as conformance and alignment, are also used and may apply to artifacts in the DoD EA. Table G-1 at the end of this appendix provides a checklist for DoD EA compliance. The following sections describe specific compliance requirements for the DoD EA.

2.1 Compliance with DoD IEA

DoD architectures for systems, services, or solutions that interact with or are part of the IE must comply with the DoD IEA. The DoD IEA is being developed in planned increments. When completed, it will provide a comprehensive description of the objective IE. The DoD IEA describes the IE vision in terms of operational requirements that drive the IE; capabilities needed in the IE to support operational requirements; and activities, rules, services, standards, and processes needed to provide, manage, and use the IE capabilities. Compliance with the DoD IEA requires relevant application of the activities, rules, services, standards, and processes described in the DoD IEA. It describes a process for applying the DoD IEA to architecture, compliance criteria, and an approach to demonstrate compliance with the DoD IEA.

2.2 Conformance with the DoD Architecture Framework

DoD Components are expected to conform to the DoDAF to the maximum extent possible in development of architectures within the Department. Conformance ensures information, architecture artifacts, models, and viewpoints can be shared with common understanding. This

promotes reuse and supports federation within the DoD EA. DoDAF conformance is achieved when:

- The data in a described architecture is defined according to the DoDAF Meta Model (DM2) concepts, associations, and attributes
- The architectural data is capable of transfer in accordance with the Physical Exchange Specification (PES); this requirement will apply once the PES is fully implemented and once DM2 and PES conformant tools are available

2.3 Architecture Registration Requirements

DTM 09-013, *Registration of Architecture Description in the DoD Architecture Registry System (DARS)* mandates the registration of architectures through the DARS portal so these architectures can be leveraged as information assets. Architectures are registered in the DARS by completing a template that is populated with content from the AV-1. Architectures developed in the DoD are more easily leveraged when they are widely visible and accessible across DoD. Widely visible and accessible architectures result in increased information sharing, reuse, and a more common understanding of the bigger picture. A fully federated EA can only be realized if all architectures in DoD are properly registered in DARS with appropriate links and relationships. DARS is located at https://dars1.army.mil/IER2/and includes a tutorial for the registration process.

2.4 Compliance with Relevant Governing Artifacts

Architecture must comply, conform, or align with guidance and direction as prescribed from all relevant governing artifacts. These artifacts include Laws, Regulations, and Policy; strategic guidance; authoritative architecture; and technical direction. Ideally, relevant content in higher-level artifacts is incorporated in more detailed content in lower-level artifacts. The intent is that consideration of all relevant information can be accomplished by complying with a few key artifacts at the lowest-level possible. To assist users in determining which artifacts are relevant to their architecture, the DoD Chief Information Office (CIO) is developing a documentation framework that categorizes and relates governing artifacts. Additional information for each set of artifacts is provided in the following sections.

2.4.1 Laws, Regulations, and Policy

Architecture must adhere to relevant content in Federal Laws and Regulations and DoD Directives and Instructions. Relevant content in Laws and Regulations are often reflected in DoD Policy, but this is not always the case. Content considered relevant to a given architecture is dependent on the purpose and scope of the architecture.

2.4.2 Strategic Guidance

Architecture must align with strategic direction described in DoD strategic artifacts as appropriate. These include artifacts such as the National Military/Defense Strategies, Operations Concepts, DoD Strategic Plans, Net-Centric Strategies, and Strategic Architecture like the DoD IEA, Business Enterprise Architecture (BEA) (*http://www.bta.mil/products/bea.html*), and Defense Intelligence Information Enterprise (DI2E) (*https://www.intelink.gov/wiki/Defense_Intelligence_Information_Enterprise*).

2.4.3 Relevant Authoritative Architecture

Solution architecture must comply with approved relevant architectures. These approved relevant architectures include higher-level architectures such as enterprise, segment, and reference architectures that are officially approved and address focus areas relevant to given solution architectures. The generally accepted hierarchy of architecture within DoD is enterprise architecture such as the BEA, Air Force EA, and DoD IEA; segment architecture such as Command and Control (C2) Capability Architecture, Logistics Architecture; Reference Architecture such as Enterprise-wide Access to Network and Collaboration Services (EANCS) RA, Active Directory Optimization RA (ADORA), and Information Technology Infrastructure Optimization RA (ITIORA); and Solution Architecture. Eventually, a IEA Information Reference Resource (I2R2) will be provided to assist in identifying relevant authoritative architecture. The intent is that relevant information from higher-level architecture gets incorporated into lower-level architecture with increased detail resulting in reference architectures that contain all relevant information. This information includes descriptions of the principles, rules, activities, functions, processes, patterns, services, systems, and standards that are applicable to solution architecture. By default, complying with reference architectures leads to compliance with all relevant authoritative architectures.

2.4.4 Technical Direction

Architecture must comply with DoD technical direction. Technical direction may be provided in the form of policy and as content in other architectures, especially reference architectures. These artifacts are addressed in other compliance criteria. The technical direction in this section is provided by the DoD Information Technology Standards and Profile Registry (DISR) and GIG Technical Guidance (GTG) and Profile (GTP). The IEA Information Reference Resource (I2R2) is also provided to assist in identifying relevant technical direction.

2.4.4.1 DoD Information Technology Standards and Profile Registry (DISR)

DoD architectures must incorporate applicable standards from the DISR. This is a DoD requirement that extends to the DoD EA. The DISR is the online repository of standards that are to be used within DoD as the "building codes" for all systems. The standards are intended to facilitate interoperability and integration of systems within DoD. DISR can be accessed at: *https://gtg.csd.disa.mil/*.

2.4.4.2 GIG Technical Guidance (GTG)and Profiles (GTP)

DoD architectures must adhere to the guidance provided in the GTG and apply standards as prescribed in approved GTPs. Application of standards per GTPs further increases interoperability and integration among services and systems.

2.5 Compliance with Mandatory Core Designated DoD Enterprise Services (ES)

Mandatory Core Designated DoD Enterprise Services are common, globally-accessible services designated by the DoD CIO and mandated for use by all programs and initiatives. No capability comparable to the Mandatory Core Designated DoD ES is to be developed unless granted by the DoD CIO. The DoD IEA provides details on how an IT program can demonstrate adoption of Mandatory Core Designated DoD Enterprise Services.

For the authoritative list of Designated DoD Enterprise Services, visit the ESRG web site at *https://www.intelink.gov/wiki/ESRG_Designated_DoD_Enterprise_Services* .

2.6 Use of Shared Designated DoD Enterprise Services (ES)

Shared Designated DoD Enterprise Services (ES) are common, globally-accessible services to be used by programs and initiatives to the maximum extent possible before consideration of alternative solutions. While use of Shared Designated DoD ES is preferable, no waiver is required when an alternative solution is used.

For the authoritative list of Shared Designated DoD Enterprise Services, visit the ESRG web site at *https://www.intelink.gov/wiki/ESRG_Designated_DoD_Enterprise_Services*.

Table G-1 - DoD Enterprise Architecture (EA) Compliance Checklist

Compliance Criteria	Description	Compliant (Yes or No)	Description of Compliance	Rmks
1. Compliance with the DoD IEA	Apply relevant rules, activities, services, standards, and IE capability guidance.			
2. Conformance with the DoDAF	Define architecture data according to the DoDAF Meta Model (DM2) concepts, associations, and attributes.			
	Make architectural data capable of transfer in accordance with the Physical Exchange Specification (PES).			
3. Registration in DARS	Register architecture in DARS with appropriate links and associations.			
4. Compliance with Relevant Governing Artifacts	Comply, conform, and align architecture with guidance and direction from all relevant governing artifacts.			
4a. Laws, Regs, and Policy	Adhere to relevant content in Federal Laws and Regulations and DoD Directives and Instructions.			
4b. Strategic Guidance	Align architecture with strategic direction described in DoD strategic artifacts.			
4c. Relevant Authoritative Architecture	Comply with approved architectures that directly bear on or constrain subject architecture .			
4d. Technical Direction	Comply with DoD technical direction in			

		the DISR, GTG and GTP.			
	4d(1). DISR	Incorporate applicable standards from the DISR.			
	4d(2). GTG/GTP	Adhere to the guidance provided in the GTG and apply standards as prescribed in approved GTPs.			
5. Compliance with Mandatory Core Designated DoD Enterprise Services		Mandated use of Mandatory Core Designated DoD Enterprise Services as prescribed.			
6. Use of Shared Designated DoD Enterprise Services		Use Shared Designated DoD Enterprise Services to the maximum extent possible.			

Appendix H: Detailed IE Operational Requirements

This Appendix describes in more detail what a warfighter, business, and/or defense intelligence operator requires from the IE to enable mission success. In Version 2.0 of the DoD IEA it contains the Core Characteristics of the IE as provided by the GIG 2.0 ORA – essentially the Warfighter requirements for the IE.

Warfighting Mission Area

For the warfighting mission area, the detailed IE requirements are organized around the core characteristics, operational outcomes, and how current IT capabilities should be transformed to achieve the described end-state as described below:

H.1 Global Authentication, Access Control, and Directory Services

The Global Authentication, Access Control, and Directory Services core characteristic encompasses several major aspects: identity and credential management, user authentication, user authorization and access control, and provision of an enterprise directory and associated services. The desired operational outcomes are:

- All authorized entities have one identity and universal credentials that are recognized by all producers of information and services
- All authorized entities have timely access to critical data, services, and applications from anywhere across the IE
- Enterprise-level directory services preserve cross domain security while satisfying information transfer requirements

Central to achieving these outcomes is the need for optimizing current operations in this area, as illustrated in **Figure H.1-1**. Optimization is achieved by streamlining identity information repositories (information resides today in multiple repositories due to a combination of disparate networks and lack of a common security framework), security frameworks, and credential authorization processes, and by ensuring that contact information is available for counterparts in other organizations, as appropriate. Identities should be provided for all authorized entities, to include DoD, Intelligence Community, and coalition partner personnel, as well as elements of the infrastructure, such as servers, unmanned aerial vehicles, and handheld devices.

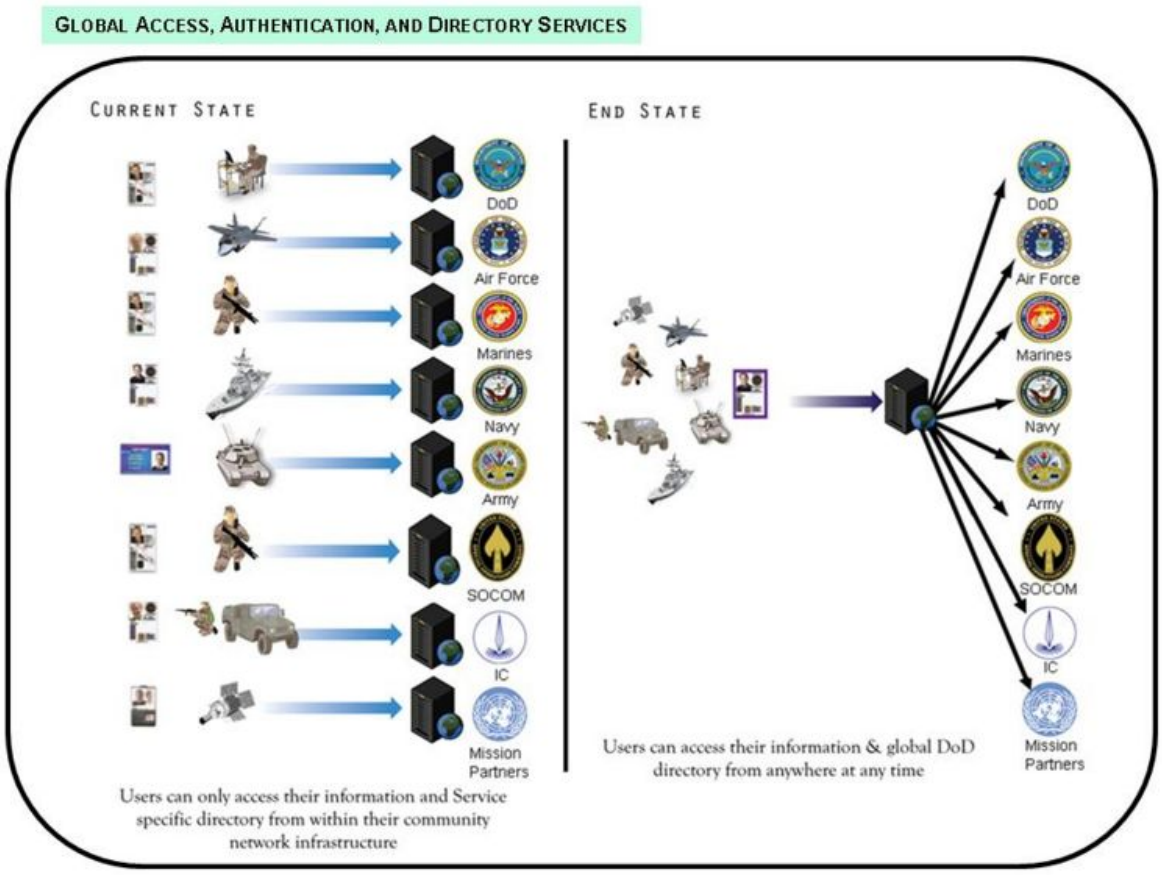


Figure H.1-1 **- Desired End-state for Global Authentication, Access Control, and Directory Services**

Identities should be tied to universal, portable credentials. Today, credentials are not consistently honored between organizations, resource owners must often implement manual methods to control access, and contact information is not readily available for counterparts in other organizations, resulting in significant delay to the warfighter, which must be overcome to ensure a sustainable military tempo and to drive innovative joint operations.

The realization of these operational outcomes will support the overall goal of providing the warfighter, business, and defense intelligence user with single sign-on access to all required information and services, regardless of location. It will ensure that commanders are confident in the fact that their units have access to the information and services needed to conduct their missions while maintaining the appropriate level of security on mission-critical information and information assets.

H.2 Information and Services "from the Edge"

The principal focus of this characteristic is to provide the deployed joint warfighter and supporting business and defense intelligence elements with the information and services they require, anytime and anywhere to achieve their mission. As envisioned, the Information and Services "from the Edge" characteristic enables three operational outcomes:

- Tactical edge users are the initial focus for requirements of any operational support activity or program development
- Data is tagged to support improved access security and rapid smart-push to the edge user based on location, community of interest, and mission
- Edge users have direct information sharing capabilities (which include the ability to share data and knowledge) with peers in and outside their immediate organization, with central processing for their mission, and with strategic assets per their mission requirements.

Figure H.2-1 provides an overview of the current and desired end-state conditions for this characteristic. Today the focus is on developing services that support DoD's business processes in the continental United States and other fixed site locations, as opposed to developing them to support the forward user. These services are then modified and pushed to tactical edge users where they are often incompatible with changing environmental factors, and as a result, are denied to consumers because they simply cannot function within a bandwidth-constrained, deployed network.

These obstacles limit battlespace awareness, speed of decision making, and the ability to access critical data. Tactical edge users must be able to discover, access, and use information assets as needed to achieve mission success instead of relying on entities far away from the operational environment to determine their information needs for them.

To accomplish this, information and services must be developed for the warfighter first to ensure they have timely assured access to the information and services required to achieve their mission goals. All services, service levels, and service delivery systems must be designed, implemented, and sustained to support warfighting functions and military operations, while also supporting DoD/Service-unique business processes. The end-state refocuses the way IT capabilities are developed by providing core information and services "from the Edge" through operations, user-centric planning, and architecting. By making tactical edge users the initial focus for requirements of any operational support activity or program development, the IE can provide seamless access to information and services that are trusted, discoverable, and available to the warfighter in order to make informed decisions.

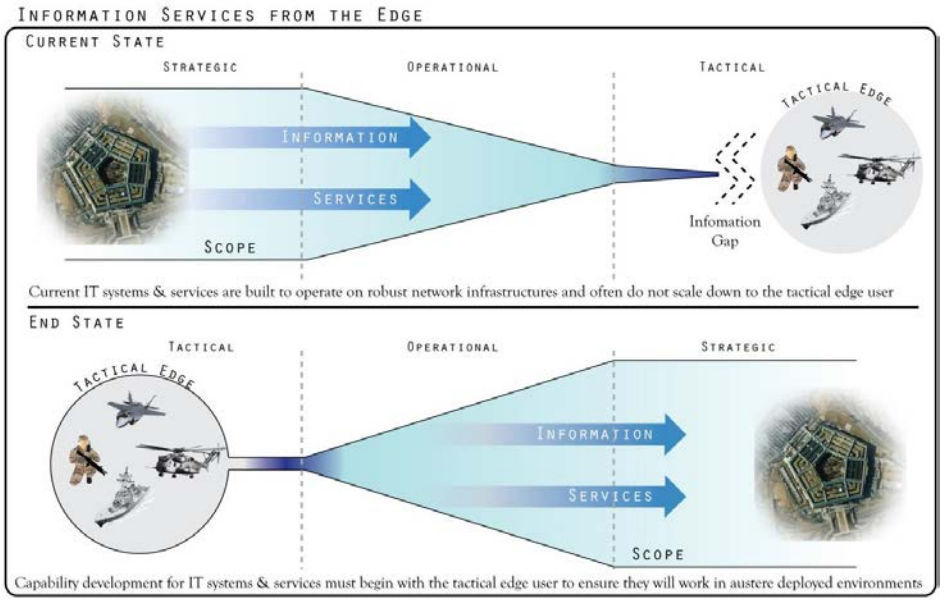


Figure H.2-1 – Desired End-State for Information and Services "from the Edge"

H.3 Joint Infrastructure

This core characteristic provides a unified information environment that interconnects IE users securely, reliably, and seamlessly. One of the recognized shortfalls in the current IE is the perpetual existence of disparate network, processing, and storage infrastructures across the DoD. This mixed environment impedes both internal and external collaboration and places warfighters and their support at the seams. The desired operational outcomes of this core characteristic are:

- Consolidated infrastructure enabling seamless information sharing and increased speed of action
- Shift away from a Military Service-centric network construct to a joint, operationally-focused construct
- A self managed computing infrastructure limiting the need for human intervention and enabling the optimization of computing infrastructure resources

Figure H.3-1 provides an overview of the current and desired end-state conditions for this characteristic. Existing infrastructures across the DoD have been built to be compliant with federal and departmental regulations while serving specific needs relevant to particular DoD missions. They are based on their own unique requirements, resulting in disparate and proprietary networks which may be inaccessible and unusable by other DoD Components, external agencies, or mission partners. This requires outside entities to negotiate separately with each DoD component to meet that particular network or systems risk profile in order to gain access to vital information and services. These burdens do not aid in the shift from a "need to know" to a "need to share" environment and severely limit the effectiveness of the joint warfighter.

In order to reach the desired end-state, the IE needs to shift away from today's Military Service-centric network construct to an operationally-focused one where the joint warfighter (Combatant Command Commander [CCDR], Joint Force Commander) is more than an integrator and Service, coalition, combined force, and interagency networks are seamless. The vision of this core characteristic is that the edge user is always included by integrating previously stove-piped structures through a unified, joint infrastructure. This consolidated, joint infrastructure will enhance mission effectiveness by ensuring data is accessible and distributed across all DoD Components and mission partners, as appropriate.

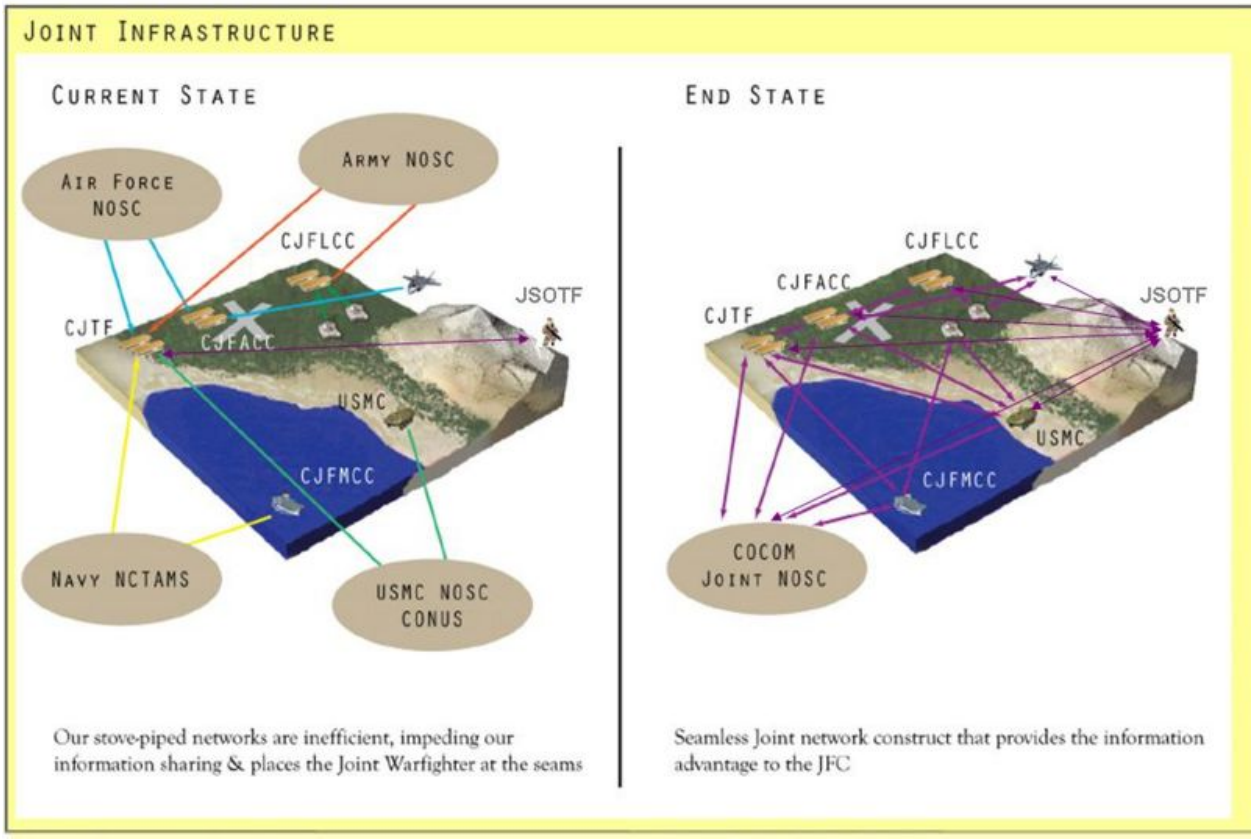


Figure H.3-1 - Desired End-State of Joint Infrastructure

H.4 Common Policies and Standards

Implementing and enforcing common policies and standards is required to ensure that the Commander's intent and goals are universally understood by an effective and unified force and the mission succeeds. The desired operational outcomes of this core characteristic are:

- Effective enterprise guidance mandating the fielding and management of IE and its infrastructure

- Enterprise acquisition and certification to ensure IE components are purchased, acquired, interoperable, and universally certified
- Common standards and policies serving as the basis for interoperability
- Reduced training requirements for end-users and IE operations personnel

Figure H.4-1 provides an overview of the current and desired end-state conditions for this characteristic. Currently, military forces continue to procure, equip, and train based on Service-centric policies and standards, resulting in disparate systems, services, and applications preventing DoD from achieving a seamless and integrated force. The current state is an environment where the infrastructure for a task force is disjointed, systems are not built to a common set of standards, and stove-piped processes implement different configurations due to the lack of governance and policy enforcement across DoD.

Implementation of the desired end-state for this core characteristic moves DoD away from a disjointed environment to one where common policies and standards serve as an enforcement mechanism to influence force integration and IT capability development. The end-state provides a unified system of policies and standards that encompass the combatant commands, Services, agencies, and mission partners and allows for information systems that are developed, tested, certified, and deployed with built-in enterprise-wide interoperability and security. A common policy and standards-based approach enables operational components to be linked through a single, secure, and unified information environment, and eliminates barriers to effective joint operations by ensuring networks, services, and software are interoperable and secure from the start. This provides Commanders and mission partners the ability to seamlessly integrate and operate IT and network capabilities in support of DoD operations.

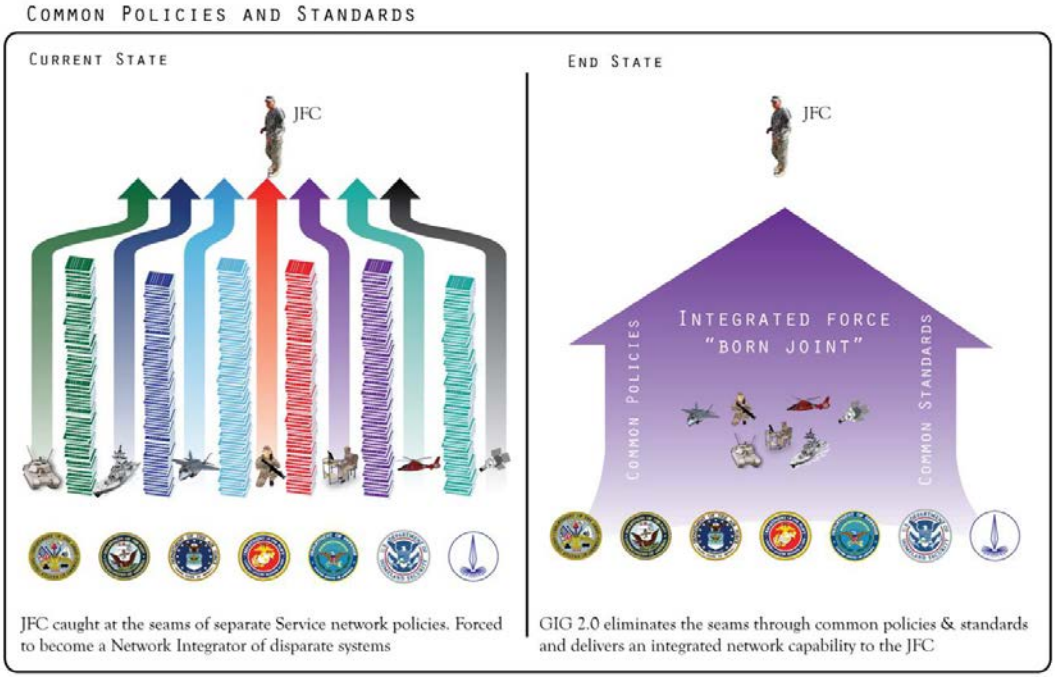


Figure H.4-1 - Desired End-State of Common Policies and Standards

H.5 Unity of Command

Improving unity of command across the IE can alleviate problems currently presented by the disjointed and stove-piped networks and policies deployed and implemented across DoD. Addressing identified Unity of Command capability gaps removes the need for Joint Force Commanders (JFCs) to act as integrators of incompatible information systems and allows for increased focus on the execution of assigned missions. The desired operational outcomes of the Unity of Command core characteristic are:

- Assured system and network availability, information protection, and information delivery providing the right information to the edge
- Effective command and control of the IE through situational awareness of a seamless information environment
- A more agile and integrated force by means of a unified training approach

Figure H.5-1 provides an overview of the current and desired end-state conditions for this characteristic. In the current IE, JFCs have limited Network Operations (NetOps) visibility and situational awareness due to varying network configurations, certification testing, and risk management procedures. Additionally, differing IT standards, network training, and management processes cause the JFC to play the role of a network integrator and to operate reactively rather than proactively when integrating forces to support operational missions. These problems result in underutilized network resources, disparate NetOps processes, and increased risk for the DoD as a whole.

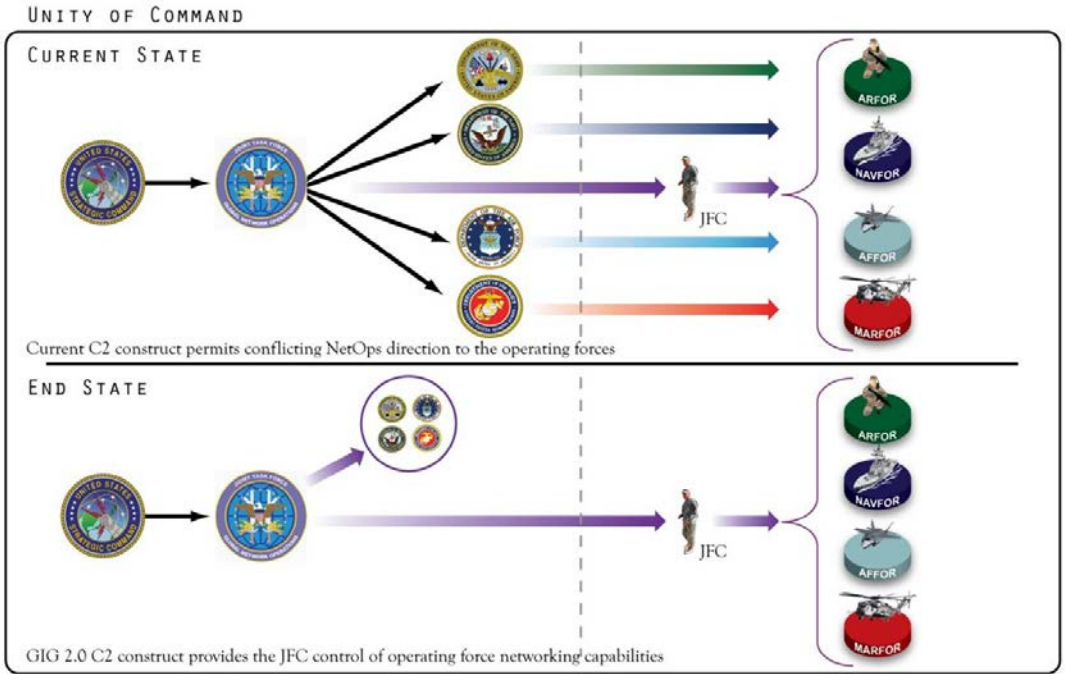


Figure H.5-1 - Desired End-State for Unity of Command

The end-state of this effort is to ensure that Military Services comply with NetOps direction provided by Cyber Command (CYBERCOM), which in turn, coordinates with the respective geographic or functional Combatant Commanders. This will enable unified support to the single commander responsible for operations and defense of the IE. Implementation of this core characteristic will eliminate seams between Services and tactical edge users by providing identical command and control (C2) structures for the IE, regardless of operational level. This includes whether units are home based or forward deployed and by proactively identifying service-impacting events in a standard and uniform manner across the DoD network infrastructure. Overarching policies and standards for NetOps will serve as an enforcement mechanism to ensure that the development and implementation of NetOps C2 capabilities are consistent with policy and recognize the authorities required for joint operations.

Business Mission Area

TBS

Warfighting Mission Area

TBS

Appendix I: Use Case (Illustrative) Examples of IEA Support to Selected Stakeholders

I-1 Introduction

This section provides the reader with more details in the form of Use Cases on stakeholder use of the IEA. The Use Case descriptions below are notional or illustrative. In some cases they represent present approaches to potential use of the IEA. In other cases they are "recommended" approaches for use of the IEA. As managers begin the process of interacting with the enterprise architecture team within the CIO as they improve their decision-making information and processes, it is anticipated that the value of the IEA will be better understood and recognized value exploited across the Office of the CIO.

The architectural data in the IEA, in conjunction with tools and analysis, can provide the necessary information to make decisions and provide specification of solutions that meet IE requirements. Many of the definitions of architectural information that were previously defined in are referenced in these Use Cases to assist the reader in understanding the type of information used in the Use Cases chosen. These Use Cases also imply that a fully populated I2R2 (containing both the IEA and outside related documentation) will assist the architect or user of the IEA extract the pertinent information to guide development of IE Solutions. It is anticipated that using the I2R2 to navigate through the available IE architectural information will provide a powerful of tool to support the needs of the Office of the CIO as well as the rest of the Department. A complementary tool, the I2R2, is currently under development and evolution to meet the needs of the IEA user community and is described at: https://www.intelink.gov/sites/dodieav2/framework/default.aspx .

Please note the following terms when reading the Use cases:

- ***"Primary Actor"*** = Identifies the Actor who's goal is being satisfied by this Use Case and has the primary interest in the outcome of this Use Case
- ***"Stakeholders and Interests"*** = Lists the various entities who may not directly interact with the Actors in the Use Cases but may have an interest in the outcome of the use case. Identifying stakeholders and interests often helps in discovering hidden requirements which are not readily apparent or mentioned directly by the users during discussions.
- ***"Extensions"*** = Extensions are branches from the main flow to handle special conditions. They also known as Alternate flows or Exception flows. For each extension reference the branching step number of the Main flow and the condition which must be true in order for this extension to be executed is described. It also highlights the high degree of integration present between various DoD CIO activities.

I-2 Architecture Development Support

I-2.1 Use Case: Identify and Develop Reference Architecture (RA) Description

Description:

A Solution Architect requests additional guidance/direction in order to deliver one or more interoperable enterprise solutions within the IE and address an operational issue, problem, or gap. The DoD EA governance body determines this guidance/direction should be in the form of a DoD-wide RA. The DoD EA governance body sets the basic purpose and scope of the RA and tasks an RA development team. The RA development team builds the RA in collaboration with Subject Matter Experts (SMEs) and other stakeholders. The DoD EA governance body then approves the RA for use across DoD and the RA is incorporated into the DoD IEA.

Primary Actor

Solution Architect

Supporting Actors

DoD EA governance body, RA development team

Stakeholders and Interests

1. DoD CIO – Has an interest in ensuring RA represents CIO's vision for DoD IE, as described by DoD IEA, and effectively provides direction/guidance CIO wishes to give solution developers
2. DoD Enterprise Architect – Has an interest in ensuring RA is aligned with and based on DoD IEA and in incorporating RA into DoD IEA
3. RA Owner – Has an interest in ensuring the RA has the correct content and in providing subject matter expertise required to properly develop RA to level of detail needed to supply proper guidance/direction

Pre-Conditions:

Approved DoD IEA must exist and contain effective architecture descriptions for required IE capabilities addressing the problem.

Post Conditions:

Success end condition

RA provides technical guidance to solution developers, in form of strategic purpose, principles, technical positions, patterns, and vocabulary, allowing delivery of interoperable solutions to satisfy identified need.

Failure end condition:

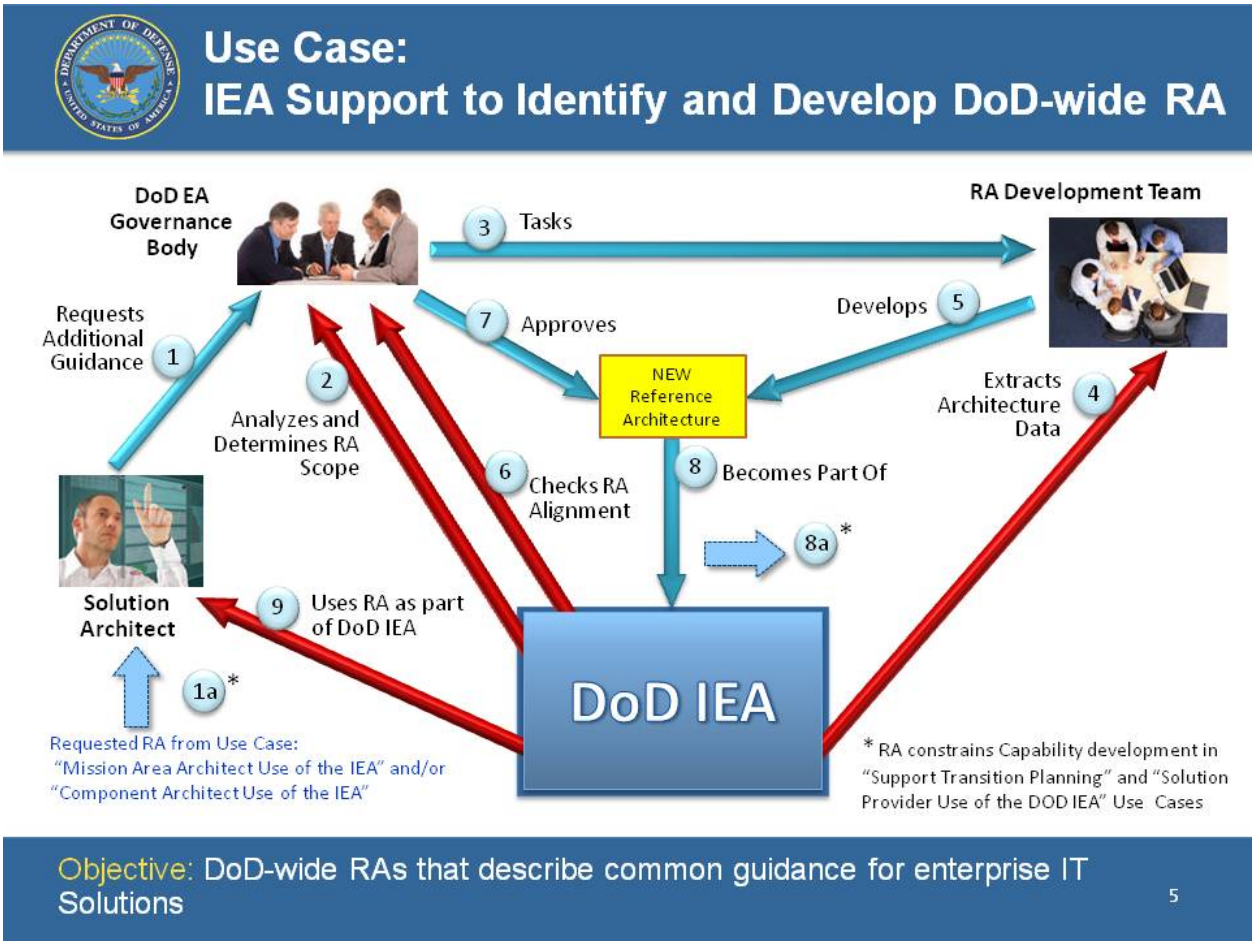
Solution developers do not receive required technical guidance at level of detail necessary to ensure interoperable solution implementation. Identified operational issue, problem, or gap is not effectively resolved.

Minimal Guarantee

RA will provide more detailed architecture descriptions of a specific set of capabilities that can be used in analyzing the DoD IEA in support of making investment decisions and determining solution development opportunities.

Trigger

Identified need for additional guidance from DoD CIO to enable interoperable solution development/ delivery in addressing a recognized operational issue, problem, or gap.



Main Success Scenario

1. Solution Architect requests additional guidance to ensure an interoperable IE solution can be implemented to address a recognized operational issue, problem, or gap.

2. DoD EA governance body analyzes DoD IEA to determine whether required direction/guidance should be in the form of an RA providing a template for the necessary solution and that such an RA does not already exist. DoD EA governance body establishes purpose for new RA and selects IE capabilities and associated activities, services, and rules from DoD IEA as scope and basis for new RA.
3. DoD EA governance body tasks team to develop RA.
4. RA development team extracts pertinent architecture data related to selected IE capabilities and associated activities, services, and rules from DoD IEA.
5. RA development team uses data from DoD IEA, supplemented with information provided by Subject Matter Experts (SMEs,) to develop strategic purpose, principles, technical positions, patterns, and vocabulary that form RA.
6. DoD EA governance body checks alignment of RA with DoD IEA.
7. DoD EA governance body approves RA and directs enterprise-wide compliance with it.
8. After approval, RA becomes part of DoD IEA.
9. Solution Architect uses RA as part of DoD IEA to constrain solution development.

Extensions:

Step 1a. The basis for a request to be issued by a Solution Architect may come from the Use Case: "Mission Area Architect Use of the IEA" and/or "Component Architect Use of the IEA".

Frequency: Whenever a need is identified for additional technical direction/guidance from DoD CIO.

Assumptions

1. A chartered DoD EA governance body is in place to help adjudicate planning, technical, cost, budget, and schedule conflicts for the benefit of a robust and managed IE.
2. The DoD EA governance body is able to access and analyze architecture data in DoD IEA to determine need for RA and select required IE capabilities and associated activities, services, and rules as scope for RA.
3. Subject matter expertise exists to provide accurate content to level of detail necessary to develop effective RA.

I-2.2 Use Case: Mission Area Architect Use of the IEA

Description

A Solution Architect responds to the requirements provided by the Mission Area EA. As part of generating the requirements for a Solution, the Mission Area (MA) EA is influenced by the

relevant "touch points" between the MA EA and the IEA. In addition, the MA EA provides requirements for the IE to support the MA. This information is then passed to the Solution Architect who retrieves relevant Capabilities provided by the IE. The resultant Solution architecture may be submitted for IEA Compliance evaluation, if it requires interaction or interoperation with the IE supplied components.

Primary Actor

The primary Actor is the Solution Architect supporting the Mission Area

Supporting Actors

The Mission Area Enterprise Architect

Stakeholders and Interests

- The Component Developers (e.g., DISA, Army Navy, etc.) have an interest in the Strategic Plan for Enterprise-wide common capabilities that the IE will supply in order to adequately address their planning needs to support DOD Missions
- The DoD EA governance body provides technical and operational guidance on the development and management of evolution of the IEA as well as Mission Area EAs and Component EAs

Pre-Conditions

A Mission Area has determined the need for development of Mission Area services and/or systems that require a Solution Architect to develop a solution to a mission need. The Mission Area EA is the source of those requirements and an approved DoD IEA is in place to support the overall requirements effort that is required to engage with a Solution Architect.

Post Conditions

Success end condition

The Solution Architect has generated a Solution Architecture that meets the needs of the Mission Area.

Failure end condition:

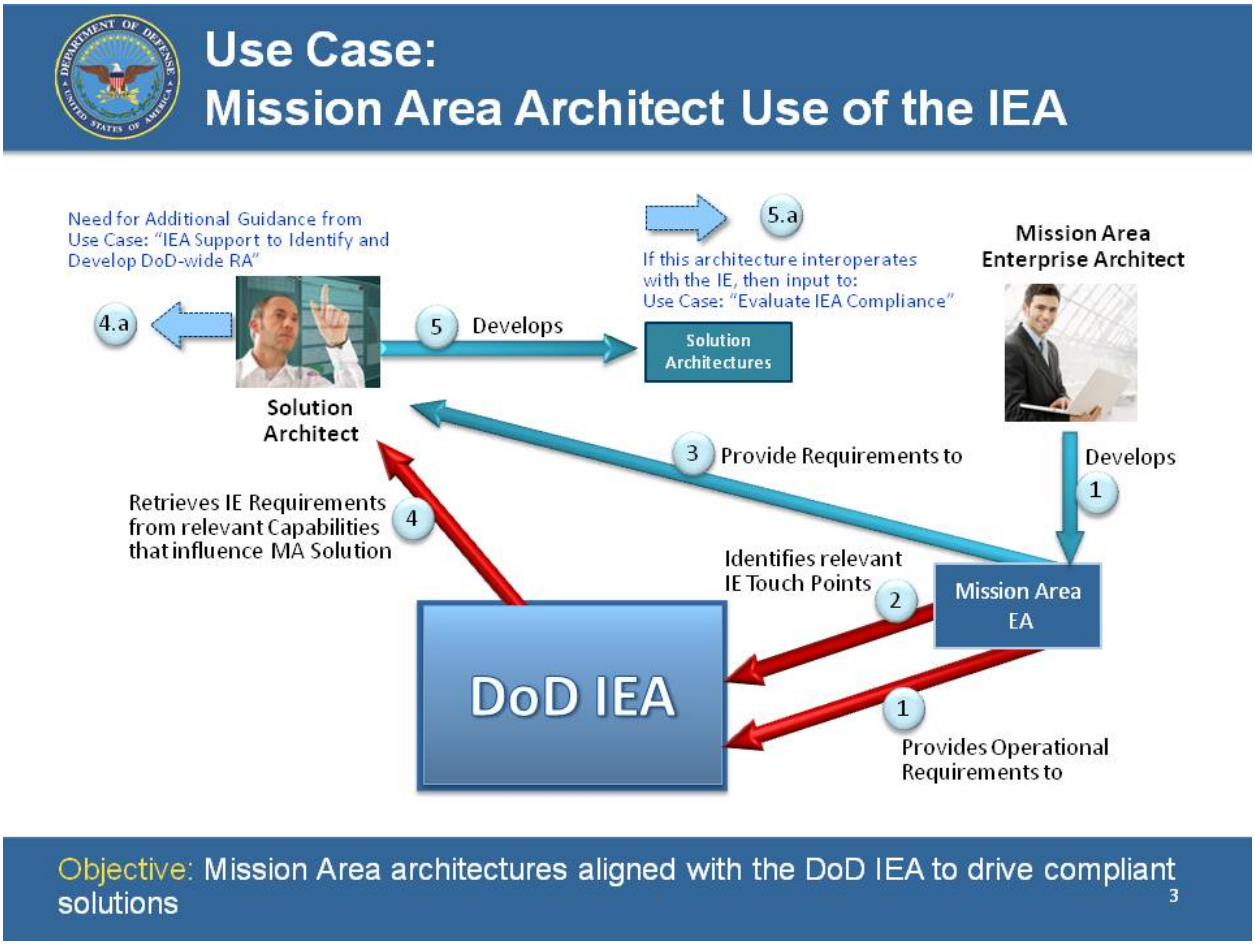
The Solution Architect has developed a Solution Architecture that is compliant with the MA EA but does not use the IEA appropriately to develop the Solution Architecture

Minimal Guarantee

An approved Solution Architecture will be compliant with the MA EA and if it uses components of the IE to interoperate or integrate with, it will need to be approved for DOD IEA Compliance in order to proceed with development.

Trigger

The initiation of a request from the Mission Area to develop a Solution Architecture.



Main Success Scenario

1. The Mission Area Enterprise Architect develops the Mission Area (MA) Enterprise Architecture (EA) and subsequently generates operational requirements for the IE. The IEA considers these in generation of the IEA, in order to meet the needs of the user community. The requirements from all Mission Areas and the DoD CIO goals are integrated into an enterprise-wide set of IE Requirements that make up the IEA. The IEA is the result of normalizing and consolidating the inputs from a group of Stakeholders that include the Components and Mission Areas.
2. The Mission Area Enterprise Architecture will evaluate the resultant IEA; identify the touch points between the Mission Area and the IE as described by the IEA in terms of Capabilities and relevant attributes. These touch points become a part of the Mission Area Requirements.
3. The Mission Area (MA) Enterprise Architecture (EA) provides the requirements for the Solution Architect to consider in development of a responsive Solution Architecture.

4. The Solution Architect will retrieve IE architecture information from the IEA pointed to by the MA EA to understand what IE requirements and architecture elements will constrain the Mission Area architecture being addressed.
5. The Solution Architect develops a Solution Architecture to address specific Mission Area needs.

Extensions

Step 4a. As a result of evaluating requirements from the Mission Area EA, the Solution Architect, generates a request for additional guidance (due to lack of architectural details from the existing evaluation of IEA requirements) which is submitted to the Use Case: "IEA Support to Identify and Develop Enterprise-wide RA".

Step 5a. The Solution Architecture may contain elements that are only unique to the MA. If they contain elements that leverage, must be shared with, or interoperate with the IE, the resultant Solution Architecture needs to comply with the IEA. If this is the case, the Solution Architecture must be submitted to the Use Case: "Evaluate IEA Compliance".

Frequency:

This Use Case will be executed for each request for a Solution to the Solution providing organization.

Assumptions:

It is assumed that an approved DoD IEA is in place to support this scenario.

I-2.3 Use Case: Component Architect Use of the DOD IEA

Description

A Solution Architect responds to the requirements provided by the Component EA. The Component EA provides requirements for the IE to support the Component. As part of generating the requirements for a Solution, the Component EA is influenced by the relevant Reference Architecture(s) in the IEA. The resultant Solution architecture may be submitted for IEA Compliance evaluation, if it requires interaction or interoperation with the IE supplied components.

Primary Actor

The primary Actor is the Solution Architect supporting the Component EA developer.

Supporting Actors

The Component Enterprise Architect

Stakeholders and Interests

- The DoD EA governance body provides technical and operational guidance on the development and management of evolution of the IEA as well as Mission Area EAs and Component EAs

Pre-Conditions

A Component has determined the need for development of Component required services and/or systems that require a Solution Architect to develop a solution to a Component need. The Component EA is the source of those requirements and an approved DoD IEA is in place to support the overall requirements effort that is required to engage with a Solution Architect.

Post Conditions

Success end condition

The Solution Architect has generated a Solution Architecture that meets the needs of the Component.

Failure end condition:

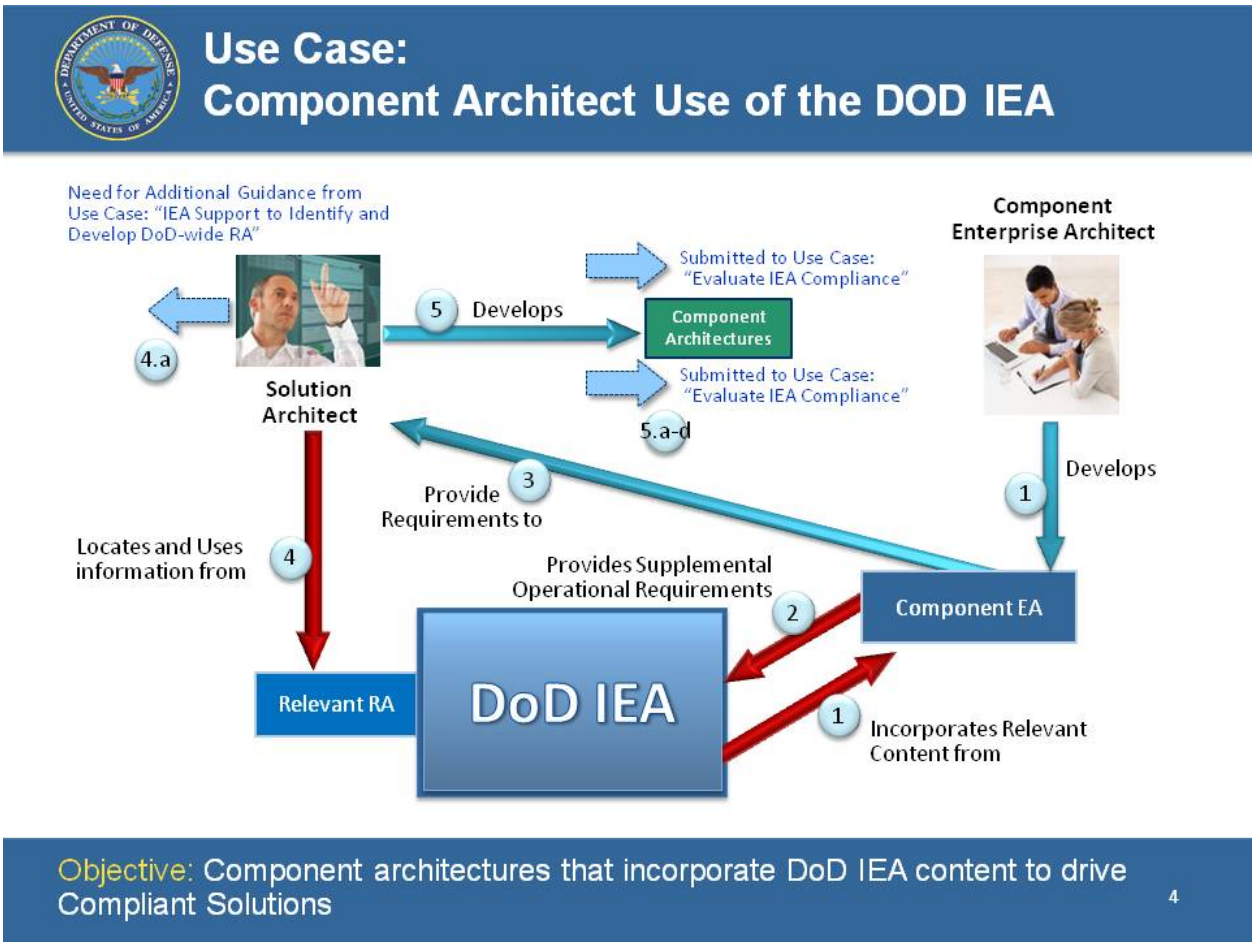
The Solution Architect has developed a Solution Architecture that is compliant with the Component EA but does not use the IEA appropriately to develop the Solution Architecture

Minimal Guarantee

An approved Solution Architecture will be compliant with the Component EA and if it uses components of the IE to interoperate or integrate with, it will need to be approved for DOD IEA Compliance in order to proceed with development.

Trigger

The initiation of a request from the Component to develop a Solution Architecture.



Main Success Scenario

1. As part of the development of the Component Enterprise Architecture will incorporate relevant content from the IEA (i.e., capabilities and their attributes).
2. The Component Enterprise Architecture will provide their supplemental requirements for support from the IE not available from Step 1.
3. Based on the requirements analysis and architecture development in Steps 1-2 above, the Component Enterprise Architecture provides the requirements for the Solution Architect to consider in development of a Solution Architecture.
4. The Solution Architect reviews the IEA for any additional IE information (primarily RAs) not provided by the Component EA (for example RAs, Rules, activities, etc.). The Solution Architect describes the resultant Component Architecture. If it contains elements that leverage, must be shared with, or interoperate with the IE, the resultant Solution Architecture needs to comply with the IEA. If this is the case, the Solution Architecture must be submitted to the Use Case: "Evaluate IEA Compliance".
5. The Solution Architect develops a Solution Architecture to address specific Component needs. It is then submitted to the Use Case: "Evaluate IEA Compliance", if it supports integration or interoperation or reuse of the IEA.

Extensions:

4a. As a result of evaluation of requirements from the Component EA by the Solution Architect, a need to develop a RA may be generated (due to lack of architectural details from the existing evaluation of IEA requirements) and would be submitted to the IE Governance Body (see Use Case: "IEA Support to Identify and Develop DoD-wide RA").

5.a – An alternate Use Case involves the alternative to step 5 which would involve responding to a request for support to a Program or Initiative where the Program management specifies Program specific IE requirements that are given to a responsible architect for a contributing solution. The Component Solution Architect will evaluate impacts on existing solutions (i.e., Steps 1-5 of this use case) that have already been developed by the Component or that is already being developed for use by the IE (under previous designated work in that Component that may be a single Capability or a set of Capabilities that encompass a previously approved IE Reference Architecture).

5.b - The resultant IE related Component Solution architecture for the IE is then described by the Component Solution Architect.

5.c Component Solution architecture is documented for approval by the Program or Initiative management.

5.d The Program or Initiative management submits the Program Specific Solution Architecture for an IE Compliance Assessment (see Use Case "DoD CIO IEA Compliance").

Frequency:

This Use Case will be executed for each request for a Solution to the Solution providing organization.

Assumptions:

It is assumed that an approved DoD IEA is in place to support this scenario.

I-3 IT Investment Management Support

I-3.1 Use Case: IEA Support to Transition Planning

Description

A normal activity under managing an enterprise according to EA development best practices is the development a of transition plan. The IE needs a transition plan to understand how it plans to evolve from its present state to one or more future states. The IEA pays a crucial and integral role to the transition planning process. In this Use Case, the staff of the DoD CIO is tasked with development of the IEA Transition Plan. They make use of the IEA to determine the future vision and compare to various factors (IE Capability Gap Priorities, Budget Guidance, As-Is

Architecture, etc.) that will influence the speed of transition to that future vision. As inputs of ongoing priorities are examined and there are conflicts with the future vision, the DoD CIO may direct changes to the IE vision (and by association the IEA) so that there is agreed upon alignment between the request for the future transition and the transition plan that will be approved by the DoD CIO. The Transition Plan will be the basis for the Programs and Initiatives that will implement the plan. The Programs and Initiatives will also require approved Investment Plan in order to finalize the resources in the planning cycle to implement the Programs and Initiatives.

Primary Actor

The primary Actor is the DoD CIO staff

Supporting Actors

The Supporting Actor is the DoD CIO

Stakeholders and Interests

- The DepSec Def has an interest in the outcome of this plan in that it supports the overall mission of the DOD.
- The Joint Staff has an interest in ensuring that the planned evolution of the IE fills the prioritized list of Capability gaps
- The Component Developers (e.g., DISA, Army Navy, etc.) have an interest in the Strategic Plan for Enterprise-wide common capabilities that the IE will supply in order to adequately address their planning needs to support DOD Components and Mission Areas
- The DoD EA governance body provides technical and operational guidance on the development and management of evolution of the IEA
- GAO has an interest in ensuring that the EA (in this case the IEA) is being used to plan how technology will be used and acquired by the DOD to support the needs of the IE over time. Although not directly interacting in this case, it has interests in evaluating compliance with Federal guidance on use of EA to drive strategic and technologic decisions for IT.
- OMB has an interest in ensuring guidelines for reporting on how EA is being used according to Federal approaches for EA development.

Pre-Conditions

In order for this Use Case to be executed, the DoD CIO staff must understand that the planned Capabilities are outlined in the IEA CV-2 description documentation. The DoD CIO staff must be made aware of the any DoD CIO directed prioritization of IE capabilities that must be supported as the IE evolves. In order to evaluate the proposed content for Initiatives/Programs the DoD CIO staff must understand to what degree the present systems and services provide the

future Capabilities desired (i.e., the As-Is Architecture). In order to conduct tradeoffs to determine the scope of Initiatives/Programs over time, the target budgets established by the DOD CIO (also allocated from the DepSec Def) must be known

Post Conditions

Success end condition

An approved Transition Plan (with their technical, cost, and schedule roadmap documented) aligned with the IEA.

Failure end condition:

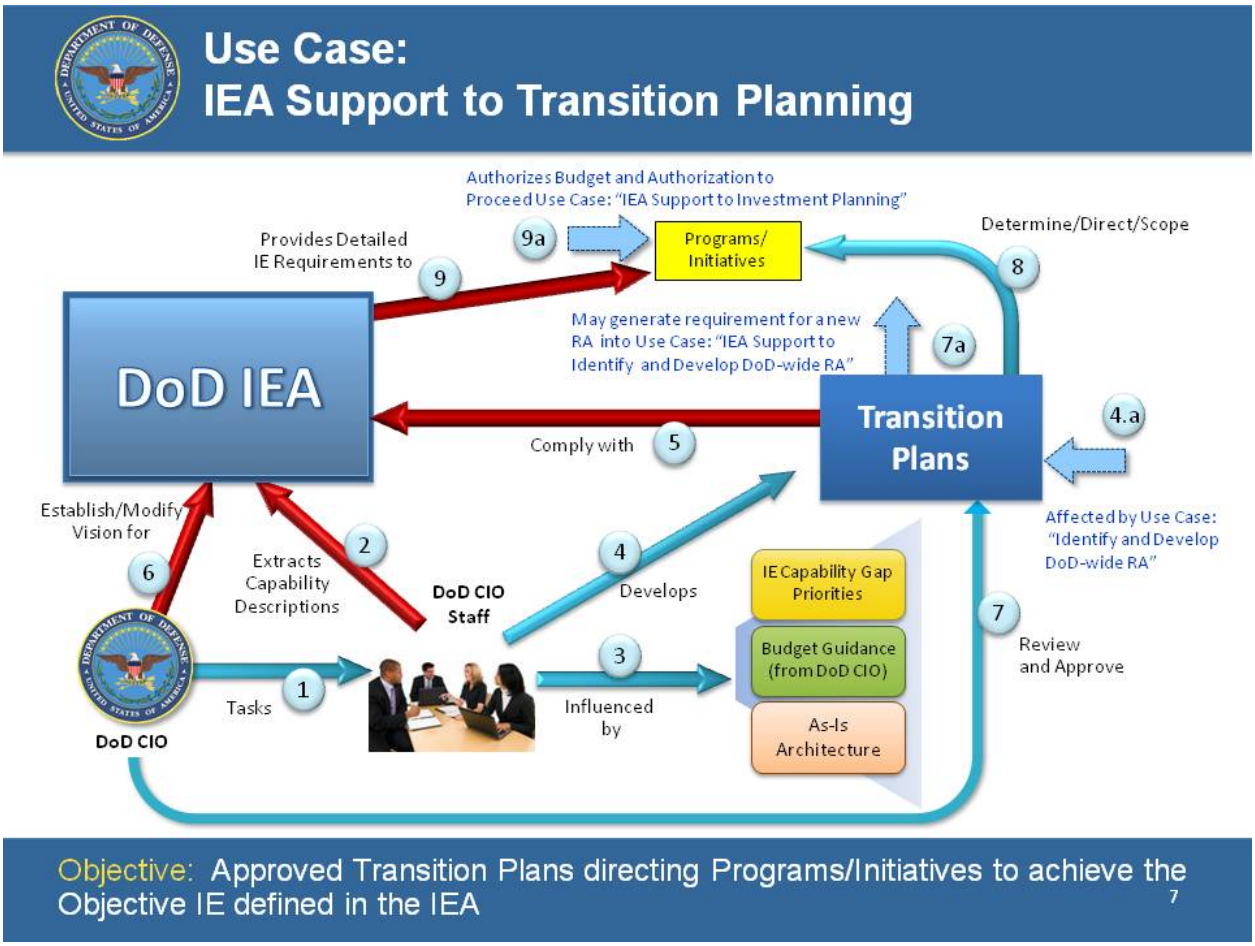
A rejected Transition Plan that need to be reprioritized or de-scoped to fit within the desired guidelines of the DoD CIO and as described in the Strategic Plan.

Minimal Guarantee

An approved DoD CIO approved Plan provides all stakeholders with sufficient guidance for detailed development and execution of the Initiatives/Programs specified in the Plan. If the IEA needs to be adjusted to better align with any changes in vision, it needs to be updated to align with the Transition Plan; the DOD CIO will direct changes to the Vision that, in turn, will precipitate an update to the IEA.

Trigger

The initiation of planning for the evolution of the IE is accomplished in concert with the DoD POM cycle as directed by the DoD CIO.



Main Success Scenario

1. The DoD CIO staff is tasked with developing a Transition Plan for evolution and transition of the IE.

2. The DoD CIO staff extracts the baselined IE Capability requirements descriptions from the Capability descriptions in the IEA.

3. The DoD CIO staff will also consider other sources of information (e.g., IE Capability Gaps, Budget Guidance, and As-Is Architecture) that effect the plan beyond just the IEA.

4. The DoD CIO staff develops the Transition Plans for vetting by stakeholders

5. The DOD CIO staff evaluates the initial draft of the Plan for Initiatives and Programs for compliance with the IEA.

6. The DoD CIO staff negotiates with DoD CIO in conjunction with tradeoffs that need to be made against budget guidance cost and priorities aligned with capability development schedules. If alignment affects potential shift in future strategy and change in capability scope and content, the CIO may designate that modification or new capabilities (update to

CV-2) be considered and would authorize changes to the IEA. This would result in alignment of IEA with the planning scope and content.

7. The DoD CIO approves the negotiated transition plan for Initiatives and Programs to be executed during the stated planning time cycle

8. The Plan now provides a basis to determine, direct, and scope the Initiatives and/or Programs to evolve the IE. This will come in the form of detailed direction on requirements for the Initiatives and Programs, but not budget authorization (which comes from Use Case: "IEA Support to Investment Planning").

9. Once the Scope and Content for the Program/Initiative has been determined, management can now extract the relevant IE requirements from the IEA to help specify the capability (or capabilities) to be developed by the Solution Providers.

Extensions:

Step 4.a - A constraint on development of a Capability to support transition plans will be the utilization of Reference Architectures (see Use Case: Identify and Develop DoD-wide RA) that may affect the scope or performance of Prioritized Capability Gaps and/or nature of Capability evolution.

Step 7.a – As part of Step 7, a need may arise to define a Reference Architecture to address the level of detail required to provide requirements for a Program or Initiative that might include multiple Capabilities in order to execute the Program/Initiative adequately. This information is fed to the Use Case: "Identify and Develop DoD-wide RA".

Step 9.a – Two parts are needed to execute a Program or Initiative. First is the Transition Plan being approved and the necessary requirements alignment with the IEA is provided as requirements. Second is the approved budget and authorization to proceed that is authorized from the Use Case: "IEA Support to Investment Planning".

Frequency:

This Use Case will be executed for each directed planning cycle as designated by the DoD CIO

Assumptions:

It is assumed that a chartered DoD EA governance body is in place to help adjudicate planning, technical, cost, budget, and schedule conflicts for the benefit of a robust and managed IE.

I-3.2 IEA Support to Investment Planning

Description

The development of a Transition Plan is the first step toward approval by an IRB to implement such a plan. An IRB will evaluate a pending Transition Plan against a set of Investment criteria.

The IRB will task an investment team to evaluate the proposed Transition Plan. The Investment Analysis Team is made up of financial and other analysts, SME, and the IE Enterprise Architect as the interpreter of the IEA and its input to and constraint on the Investment criteria for the team. The Investment Analysis Team will assist the IRB in modify and adding to the Transition Plan in order to provide inputs in the IT Portfolio. Once the IRB approves the Investment Plan, the IT Portfolio management will ensure that that the Programs/Initiatives implement the Investment Plan (reflecting the approved Transition Plan) within the scope and resources approved by the IRB.

Primary Actor

The primary Actor is the IRB

Supporting Actors

The Supporting Actor is the Investment Analysis Team.

Stakeholders and Interests

- The DoD EA governance body provides technical and operational guidance on the development and management of evolution of the IEA
- GAO has an interest in ensuring that the EA (in this case the IEA) is being developed as planned and that the performance of the Capabilities that are being acquired is being monitored, reported and plans adjusted to meet performance of the Capabilities desired. Although not directly interacting in this case, it has interests in evaluating compliance with Federal guidance on use of EA to drive strategic and technologic decisions for IT.
- The DoD CIO has an interest in ensuring that budget guidance and IE Vision provided to the CIO's staff is being implemented and followed in planning Programs and Initiatives.

Pre-Conditions

There will be an approved Transition Plan for all DoD CIO Initiatives and Programs made available to the IRB.

Post Conditions

Success end condition

Successful completion of an investment analysis in support of an IRB decision for an approved IT Portfolio. This will be used to guide Programs and Initiatives.

`Failure end condition:

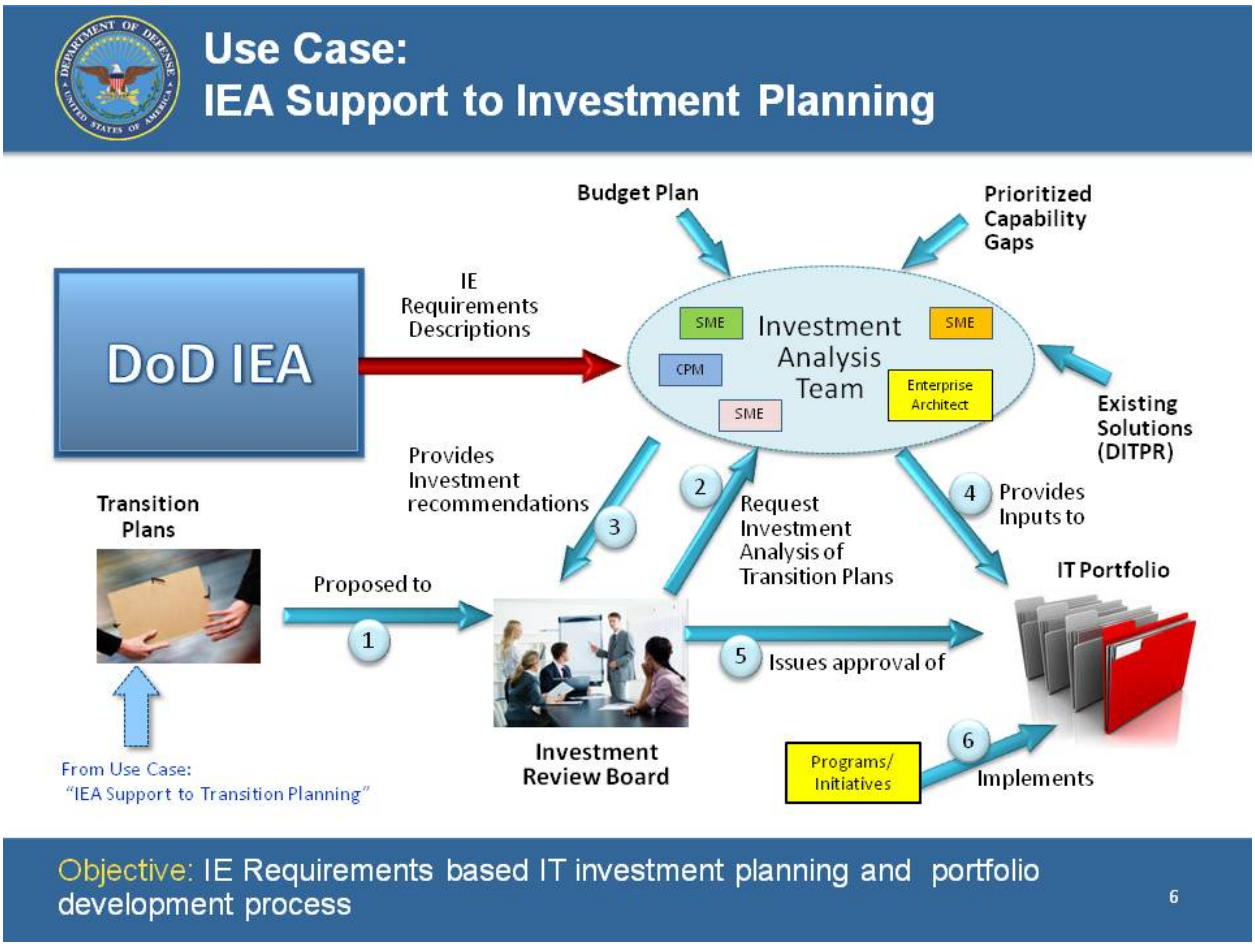
Lack of adequate Investment Plan based on the Transition Plan and constraints and criteria set by the IRB

Minimal Guarantee

The IRB will provide sufficient guidance to implement an IT portfolio representing the proposed Transition Plan.

Trigger

Receipt by the IRB of a proposed Transition Plan and associated Programs/Initiatives.



Main Success Scenario

1. The developed Transition Plans (coming from the Use Case: "IEA Support to Transition Planning") are proposed to the DoD CIO Investment Review Board (IRB).

2. The IRB request investment analysis of Transition Plans submitted to IRB.

3. An Investment Analysis Team (made up of various stakeholders; e.g., CPM; SMEs; analysts; and an enterprise architect) is convened to conduct an analysis of the Transition Plans. This team has inputs from various sources (Existing Solutions – DITPR; Prioritized Capability Gaps; Budget Plan, and the future vision for the IE contained in the

IEA amongst others. The Investment Analysis Team provides investment recommendations to the IRB.

4. The Investment Analysis Team provides the inputs to production of the IRB approved IT Portfolio. This may include changes to the original Transition Plans
5. Based on evaluation of the results of the analysis conducted by the Investment Analysis Team, the IRB issues an approval of the recommended IT Portfolio with any amendments.
6. The approved IT Portfolio provides authorization and budget to proceed on a subset of Programs and Initiatives outlined in the original Transition Plans.

Extensions:

None Identified

Frequency:

This Use Case will be executed for each directed IRB evaluation of a proposed Transition Plan.

Assumptions:

It is assumed that the IRB charter is in place. An Investment Analysis Team has been identified and its resources are made available to the IRB during a pre-negotiated timeframe.

I-4 IT Program Manager Support

I-4.1 Use Case: Evaluate IEA Compliance

Description

In order to manage and use the IE effectively to deliver consistent and common services across the enterprise an EA Governance Body needs a tool to assist in evaluation of the compliance of solution architectures to meet the goals of the IE. The IEA provides the data requirements for such a tool. The governance body will receive solution architectures (to include requested reference architectures) to evaluate for compliance with the IEA. It will engage with the IE Enterprise Architects that will assist the EA Governance Body in carrying out targeted IEA Compliance evaluations. The recommendation from the assessment will be provided to the EA Governance Body; who will then make a compliance decision on the degree of compliance with the IEA.

Primary Actor

The primary Actor is EA Governance Body.

Supporting Actors

The Supporting Actor is the Enterprise (in this case IE) Architect.

Stakeholders and Interests

- The DepSec Def has an interest in the outcome of this plan in that it supports the overall mission of the DOD.
- The Joint Staff has an interest in ensuring that the planned evolution of the IE fills the prioritized list of Capability gaps
- The Component Solution Developers (e.g., DISA, Army Navy, etc.) have an interest in the Strategic Plan for Enterprise-wide common capabilities that the IE will supply in order to adequately address their planning needs to support DOD Missions
- The Mission Area Solution Developers have an interest in the Approval of their plans for Mission Area Solution development and evolution to address their changing needs.
- GAO has an interest in ensuring that the EA (in this case the IEA) is being used to plan how technology will be used and acquired by the DOD to support the needs of the IE over time. Although not directly interacting in this case, it has interests in evaluating compliance with Federal guidance on use of EA to drive strategic and technologic decisions for IT.
- OMB has an interest in ensuring guidelines for reporting on how EA is being used according to Federal approaches for EA development.

Pre-Conditions

In order for this Use Case to be executed, a baselined DoD IEA must be in place and a plan for how IEA architects need to support the EA Governance Body needs to be approved.

Post Conditions

Success end condition

An architecture evaluated for IEA compliance has been provided to the EA Governance Body for their deliberation on the acceptability of the provided Solution architecture to integrate or interoperate with the IE.

Failure end condition:

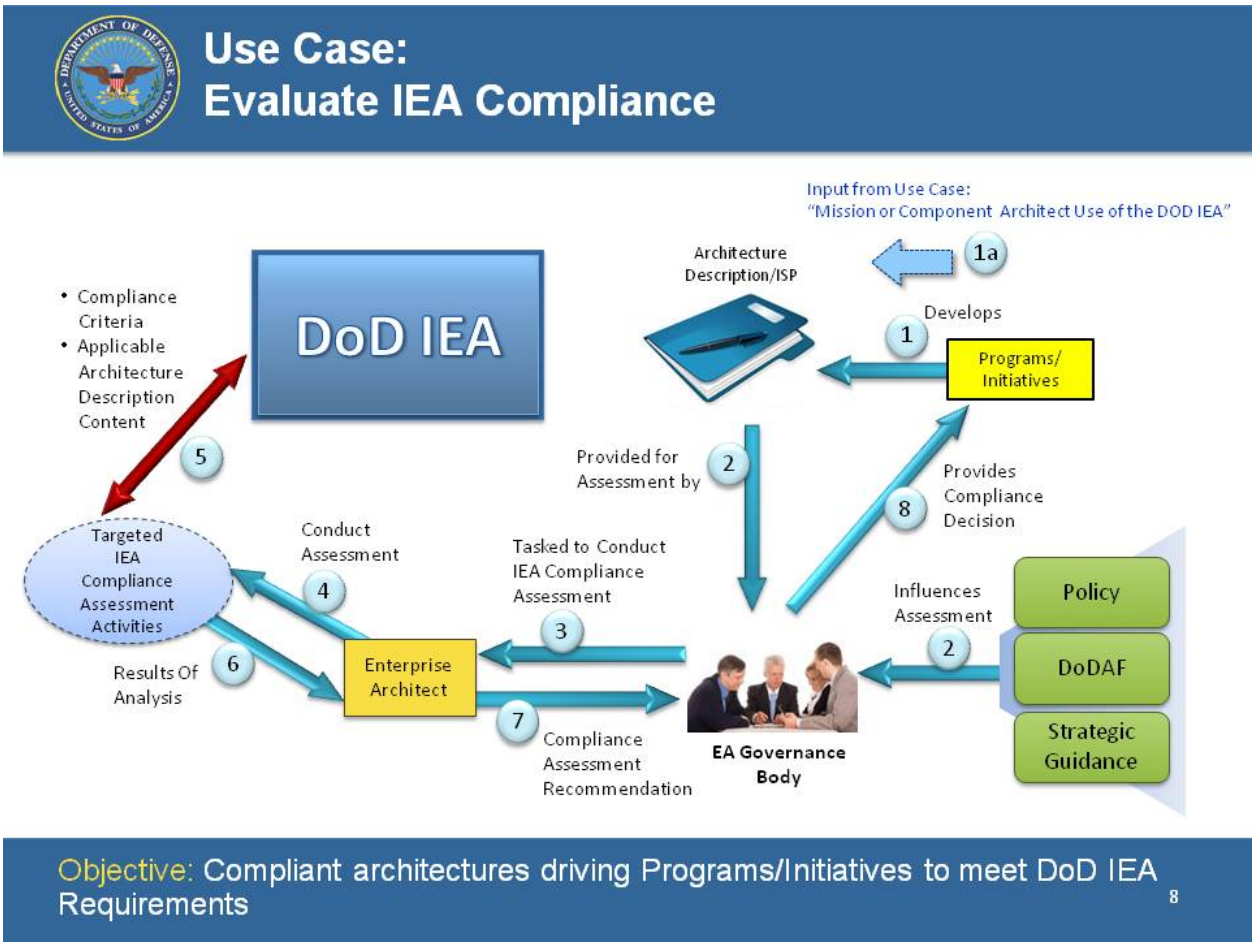
An architecture could not be evaluated for compliance with the IEA due to lack of sufficient architectural data on the submitted architecture.

Minimal Guarantee

An architecture can be evaluated for IEA compliance sufficiently for the EA Governance Body to make a decision on acceptability of the Solution architecture for compliance against IEA compliance criteria.

Trigger

The submittal of a Solution architecture (most likely through a Program or Initiative) to the EA Governance Body that needs to use, interoperate with, or integrate with the IEA.



Main Success Scenario

1. A Program or Initiative develops an architecture and/or ISP.
2. The Architecture and/or ISP is submitted for IEA Compliance Assessment to the EA Governance body. In carrying out EA governance, factors affecting oversight include: DOD Policy, DODAF compliance, and Strategic Guidance.
3. The EA Governance body will task the Enterprise Architect to conduct an IEA Compliance Assessment.
4. The Enterprise Architect will conduct the assessment using various evaluation techniques carried out through Targeted IEA Compliance Assessment Activities which depend on the type of architecture (e.g., solution architecture for a single capability or reference architecture used to combine or refine existing Capabilities defined in the IEA).

5. A set of Targeted IEA Compliance Assessment Activities will interact with the IEA using Compliance Criteria and applicable architecture description content.

6. The Enterprise Architect will review the results of the analysis.

7. The Enterprise Architect will provide the EA Governance Body with a Compliance Assessment Recommendation.

8. The EA Governance Body will review the recommendation and issue a Compliance Decision to Program/Initiative management. This will provide the Program/Initiative part of the required approvals to implement the architecture (the other part coming from the Use Case: "IEA Support to Investment Planning").

Extensions:

Step 1.a The source of the architecture to be evaluated for compliance will come from the activities accomplished in the Use Case: "Mission Area Architect Use of the DOD IEA" or "Component Architect Use of the DOD IEA".

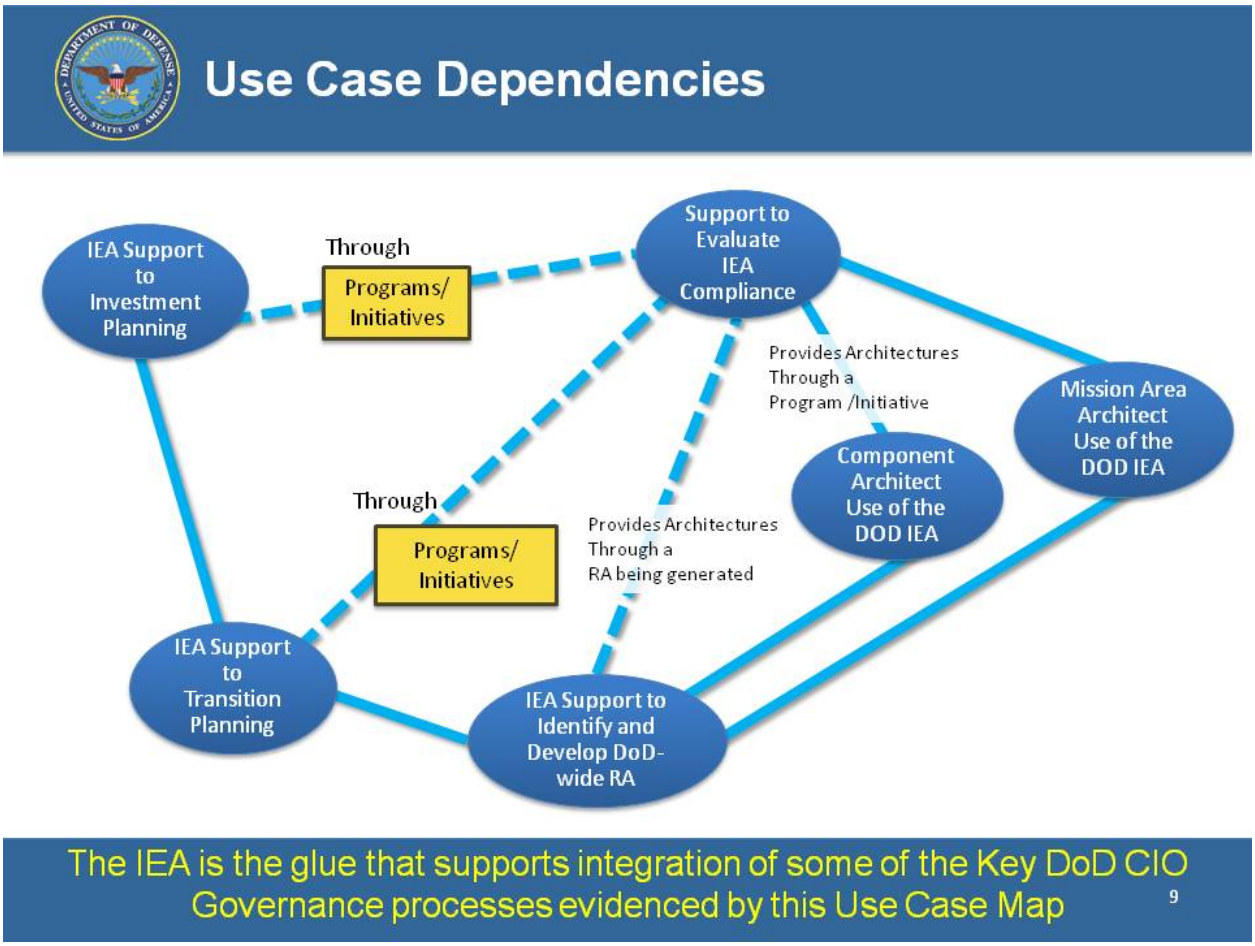
Frequency: This Use Case will be executed for Solution Architecture or RA submitted to the EA Governance Body for evaluation of IEA Compliance.

Assumptions:

It is assumed that a chartered DoD EA governance body charter support the process described here.

I-5 Use Case Dependencies

In each Use Case, linkages were shown to other Use Cases through "Extensions" in those Use Cases. It is important to note the integrating function that the IEA plays in each one of the Use Cases. As such, the IEA is central to a coherent and integrated approach to management and evolution of the IE. The following graphic, sometimes referred to as a Use Case Map, is a 20,000 foot view of these dependencies to gain a better appreciation of how governance of the IE is impacted through use and management of the IEA. The dashed lines show how Use Cases are impacted by "indirect" dependencies (e.g., through Programs/Initiatives or through RAs being generated), while the solid line connectors point to more strongly dependent Use Cases.


Use Case Dependencies
IEA Support to Investment Planning
Through
Programs/ Initiatives
Support to Evaluate IEA Compliance
Provides Architectures Through a Program /Initiative
Mission Area Architect Use of the DOD IEA
Component Architect Use of the DOD IEA
Through
Programs/ Initiatives
Provides Architectures Through a RA being generated
IEA Support to Transition Planning
IEA Support to Identify and Develop DoD-wide RA
The IEA is the glue that supports integration of some of the Key DoD CIO Governance processes evidenced by this Use Case Map
9

Appendix J: AV-2 Integrated Dictionary

This appendix contains the AV-2 for the DoD IEA in the form of an embedded Excel workbook. The AV-2 contains definitions for all activities, capabilities, and services described in the DoD IEA.

Integrated
Dictionary (AV-2)