Department of Defense Information Enterprise Architecture
Overview and Summary Information (AV-1)
May 7, 2010

This Overview and Summary (AV-1) document is an executive-level presentation of the Department of Defense Information Enterprise Architecture (DoD IEA). It was used to focus the DoD IEA development efforts.	
Architectural Description Identification	
Name	Department of Defense Information Enterprise Architecture (DoD IEA)
Architect	Department of Defense (DoD) Deputy CIO
Developed By	The DoD IEA development team within the DoD Deputy CIO organization with participation from all CIO directorates, other DoD representatives, and Components.
Assumptions and Constraints	• Content for the DoD Information Enterprise Architecture effort was provided by all DoD CIO directorates as well as key stakeholders from across the Department. • The DoD Information Enterprise Architecture is by no means complete. Given the evolutionary nature of IT development, the DoD IEA is, and always will be, a work in progress. The DoD IEA builds a foundational level of principles and rules by which the entire enterprise shall abide. These concepts must become embedded across the Department before effective DoD-wide transformation can take place.
Approval Authority	The Assistant Secretary of Defense NII/DoD CIO, acting through the DoD Deputy CIO.
Date Completed	May 7, 2010
LOE and Costs	Level of effort, projected and actual costs to develop the DoD IEA may be requested from the DoD Deputy CIO.
Scope: Architecture View(s) and Products Identification	
Products Developed	<u>DoD IEA Architecture Description</u> – Document that list the principles, rules, constraints and best practices that are part of the architecture. <u>Overview and Summary AV-1 (this document)</u> - Provides an executive-level summary of the architecture effort that clarifies the content, purpose and viewpoint of the architecture. <u>Hierarchical Activity Model</u> - Decomposes and defines the activities in the architecture. <u>Principles and Rules</u> - Provides a concise listing of principles, business rules, constraints and best practices that govern the Defense Information Enterprise. It also describes the current list of designated DoD Enterprise Services that are mandatory for use in every DoD IT investment. <u>Glossary</u> - Provides a listing and definition of terms used in the architecture.
Time Frames Addressed	DoD IEA addresses a "To Be" vision that will be used to influence the POM.
Organizations Involved	DoD IEA involves operations of the Defense Information Enterprise (led by the DoD Deputy CIO at the Enterprise level) as they relate to the four areas of net-centric operations: Enterprise Services, Information Assurance, Computing Infrastructure, and Communications. The DoD Deputy CIO, in conjunction with the DoD CIO Directors, determines architecture priorities based on the needs of the DoD.
Purpose and Perspective	

Purpose	The Department of Defense Information Enterprise Architecture (DoD IEA) provides a common foundation to support accelerated DoD transformation to net-centric operations and establishes priorities to address critical barriers to its realization. The Defense Information Enterprise comprises the information, information resources, assets, and processes required to achieve an information advantage and share information across the Department and with mission partners. DoD IEA describes the integrated Defense Information Enterprise and the rules for the information assets and resources that enable it. DoD IEA unifies the concepts embedded in the Department's net-centric strategies into a common vision, providing relevance and context to existing policy. DoD IEA empowers DoD decision-makers across all tiers and portfolios (including Investment Review Boards and Capability Portfolio Managers) in managing the overall DoD Information Technology (IT) portfolio. Components will use DoD IEA to strategically align their programs and architectures with the enterprise net-centric vision. DoD IEA addresses a "To Be" vision and will influence the Program Objective Memorandum process.
Questions to be Answered	• How does DoD enable the creation and deployment of data, information and services in a net-centric environment? • How does DoD ensure that our information resources are secure and trusted, yet accessible, across the entire DoD network environment? • How does DoD ensure our communications/computing infrastructure is adequate to the task of fully supporting global net-centric operations? • How does DoD manage and operate the GIG to ensure it is available and ready for use?
Architecture Perspective	The DoD IEA perspective is that of an Enterprise or Component CIO-level architect/decision maker. It will serve as a tool to communicate leadership's direction for DoD information technology and to drive investments to achieve that vision.
Context	
Mission	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. • An available and protected network infrastructure (the GIG) that enables responsive information-centric operations using dynamic and interoperable communications and computing capabilities.
Goals	Drive the fundamental concepts of net-centricity across all mission of the Department of Defense to ensure that all applicable DoD programs, regardless of Component or portfolio, comply with the DoD net-centric vision and enable agile, collaborative net-centric information sharing.

Information Environment	During the development of this architecture, five priorities were identified as areas where increased attention and investment would drive important progress towards achieving net-centric information sharing. These priorities are the fundamental organizational construct for the DoD IEA, and focus the architecture on aligning investments with net-centric principles. These priorities are listed below. • 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). • 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. • 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. • Communication 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. • 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.
Rules Followed	**Rules –** • The development approach assumed that a minimal, universal, common set of implementation specifications should be adhered to in order to drive net-centric transformation. • Architecture products were developed and decomposed only to the level of detail required to support investment decision-making at the DoD and Component CIO level. • The architecture represents data and services as independent from systems and applications and shows how they are made visible, accessible, understandable, trusted, and governed across the Enterprise. • The architecture documents all critical rules, constraints and best practices necessary for accelerating the implementation of net-centric operations. These are sufficiently critical and "Enterprise" in nature that waivers should be granted only in exceptional cases. • The architecture establishes enabling guidelines and standards.
Linkages to Other Architectures	DoD IEA is federated with other Enterprise (Department, Capability and Component) and Solution architectures through tiered accountability as described in the GIG Architecture Federation Strategy.
Tools and File Formats Used	
Rational System Architect, MS Word, MS Excel and Adobe Acrobat	