Department of Defense

Enterprise Architecture (EA) Modernization Blueprint/ Transition Plan

25 February 2011

Prepared by:
Director, Architecture & Infrastructure
Office of the Department of Defense Chief Information Officer

DoD EA Modernization Blueprint/Transition Plan

Executive Summary

The OMB Chief Architect requested a description of the current Enterprise Architecture (EA) Modernization Blueprint/Transition Plan for each agency to further his understanding of the status of each agency's overall EA planning. This document describes the Department of Defense (DoD) EA, the current status, and the way ahead.

The DoD is a complex organization comprised of multiple Components (Combatant Commands, Services, and Agencies) with varying missions and operations. These Components function both autonomously and as interoperable, integrated elements. A single, monolithic DoD EA cannot effectively describe all DoD components; current and future capabilities, functions, and relationships; and the varying transition strategies. It was necessary to take an approach for the DoD EA that provides an effective description of all DoD Components and relates them in some meaningful way.

DoD has taken a federated approach for developing and managing the DoD EA that is based on enterprise-level guidance, capability areas, and component architectures. A Federated DoD EA is the best way to effectively describe a complex Department and provide the necessary context and guidance to govern, manage, and accomplish the missions of the Department. This approach is described in a Federation Strategy that is currently being updated. The strategy describes an approach to enterprise architecture that facilitates interoperability and information sharing between semi-autonomous departments, components and programs. This approach recognizes the need for autonomy but requires linkages and alignment of architectures from the Program level up to the Enterprise level. A governance body and associated processes are in place to provide the necessary governance and oversight with respect to the strategy. The Governance body consists of subordinate working groups that contain Department-wide representation. Requirements for DoD EA compliance are captured in the CIO approved DoD Information Enterprise Architecture (IEA) document that is posted on the CIO public site for department-wide use.

 DoD has instituted a policy requiring the registration of architectures in a DoD architecture registry system (DARS) that provides visibility and accessibility for all registered architectures. Other architecture requirements are imbedded in various policies in the Department such as the DoDD/I 4630, DoDD 8000, CJCSI/M 3170, and CJCSI 6212. Together, these policies provide the direction needed to maximize the sharing and use of architectures in key DoD processes.

The federated approach and structure for the DoD EA is constant while the content of the DoD EA continues to change. As new architectures are approved and existing architectures are updated, the content of the DoD EA grows and matures. DoD has designated eighteen segments, aligned with the Joint Capability Areas (JCA), to guide and support IT investments and solutions in adherence with OMB guidance. The DoD EA is applied to guide investment portfolio strategies and decisions; define capability and interoperability requirements; establish and enforce standards; guide security and information assurance requirements across DoD; and provide a sound basis for transitioning from the existing environment to the future

Contents

1 DoD EA Description

As required by OMB Circulars A-11 and A-130, DoD maintains a target EA that is dynamic, changing, and expanding. Not a single, overarching artifact, the Target EA is a federation of architecture descriptions that provides context and rules for accomplishing the mission of the Department. Constituent architectures are developed and maintained at the Department, capability area, and Component levels to collectively define the people, processes, and technology required in the current and target environments. Each of the "subsidiary" architectures also provides a roadmap for transitioning a given part of DoD to a new-and-improved, target operating environment.

The DoD Enterprise Architecture (EA), depicted in **Figure 1**, is a continual work in progress. It exists today as a loosely related set of functionally and organizationally-specific architectures. EA looks at specific functions and capabilities, indicates what policies apply, and provides interpretation, highlighting the applicable policies and removing ambiguity through operational context. The DoD EA enables decision makers to look across the enterprise for gaps and opportunities for consolidation. The DoD EA will continue to be used to institutionalize consistent, effective use of architecture across the Department, strengthen the use of architecture in the key decision-making processes of the Department, including the Joint Capabilities Integration and Development System (JCIDS), Defense Acquisition System (DAS), Business Capability Lifecycle (BCL), Planning, Programming, Budgeting and Execution (PPBE), Capability Portfolio Management (CPM), and Joint Concept Development and Experimentation (JCD&E), in a manner that enables better-informed decisions.

The DoD EA itself is a federated system in which the leadership of each capability segment and Component (e.g., Military Department, Defense Agency, and Combatant Command (COCOM)) maintains its own architectural documentation and transition plan, and coordinates with all entities with which it overlaps and shares services and capabilities. Enterprise rules outline how the parts of the federation interrelate to effect optimal Department-wide performance. Each of these individual efforts is a substantial effort in and of itself. There is no plan to turn this federated environment into an integrated one in which all architectures and plans are rolled up into a single "master plan." Each of the various capability and Component transition plans are very dynamic, with widely ranging periodicity depending upon need. Links to artifacts that contain this information are provided towards the end of this document.
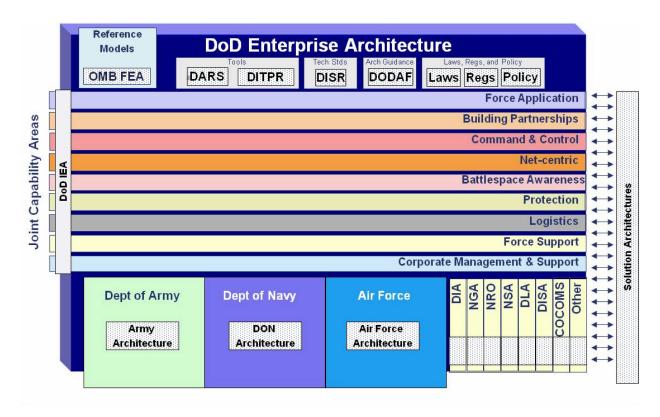
Figure 1 - DoD Enterprise Architecture (EA) Graphic

The top of Figure 1 shows the architecture tools, reference models, standards, guidance, and the laws, regulations, and policies that govern DoD's operations. These are reflected in the DoD EA as controls of various types on the business processes, business activities, business rules, IT services, IT standards applied – as well as the information/data handling by everyone – throughout the Department.

The middle of Figure 1 shows the nine Joint Capability Areas (JCAs) for the DoD. The JCAs are a standardized set of definitions that cover the complete range of the Department's mission-related activities. Initially established in 2005 by the Joint Staff with input from each of the military services, the set of JCAs was designed to facilitate side-by-side comparisons of service contributions to joint mission needs, as decision-makers address the implications of moving resources between service budgets. Other parts of the DoD EA are built and maintained by different stakeholders. The DoD has currently designated eighteen DoD Segments grouped into the three categories prescribed by OMB (Core Mission-related, Enterprise Services-related, and Business Services-related) that align with the JCAs. The DoD Segments are listed in **Table 1**.

DoD Components, shown along the bottom of Figure 1, represent enterprises unto themselves, operating within the scope of the larger DoD enterprise. Each Component has Enterprise Architecture (s), which align with that maintained by each of the other Components, to jointly support DoD missions.

Solution Architectures are not part of the DoD EA, but they are shown to the right of the diagram to indicate that solutions are guided and constrained by the architectures that make up the DoD EA. They play a key role in the DoD acquisition processes in that architecture-enabled solutions facilitate improved interoperability, better information sharing, stricter compliance, leaner processes, and result in reduced costs and more effective mission accomplishment. Solution Architecture viewpoints provide key components of the Capability Development Document (CDD) and Capability Production Document (CPD) to ensure DoD understands the linkages between capabilities and systems and can make appropriate acquisition decisions; and the performance attributes, including key performance parameters (KPPs) and key system attributes (KSAs), that define the most critical elements of performance for the systems under development.

Table 1 - DoD Designated Segments

Core Mission Segments	Enterprise Services Segments	Business Services Segments
Force Application	Identity & Information Assurance	Human Resources Management
Building Partnerships	IT Infrastructure	Logistics/Supply Chain Mgmt
Command & Control	Information Technology Management	Installation Support
Battlespace Awareness-ISR		Financial Management
Battlespace Awareness-Environment		Acquisition
Protection		
Battlespace Networks		
Force Training		
Force Management		
Health		

The DoD IEA is represented in Figure 1 by a vertical block positioned across the nine JCAs. The current Version 1.2, released in May 2010, provides the foundation for achieving the DoD Information Enterprise (IE) vision. It describes a set of principles, rules, activities, application guidance, and compliance criteria that apply to all DoD architectures. The purpose of the DoD IEA is to:

- Unify the concepts embedded in the DoD net-centric strategies into a common vision

- Drive common solutions and promote consistency

- Describe the integrated Defense Information Enterprise and the rules for information assets and resources that enable it

- Foster alignment of DoD architectures with the enterprise net-centric vision

A key addition to the DoD IEA v1.2 is an appendix (Appendix G) that describes the compliance requirements for the DoD EA. They are:

- Compliance with the DoD IEA

- Architecture Registration Requirements: DTM 09-013 mandates registration of architectures in DARS

- Compliance with Capability and Component EAs

- Compliance with DISR: All architectures must incorporate applicable standards from the DISR

- Compliance with Mandatory Core Designated DoD Enterprise Services (ES): DoD ES mandated for use by all programs and initiatives

- Use of Shared designated DoD ES: To be used by programs and initiatives to the greatest extent feasible

Together, these parts comprise the federation known as the DoD EA. Each part of the DoD EA represents a strategic, capability or component scope. Federation enables the distributed development and maintenance of the many parts.

2 Importance of Rules and Context for Applying EA

The intended use of the DoD EA is to guide investment portfolio strategies and decisions, define capability and interoperability requirements, establish and enforce standards, guide security and information assurance requirements across DoD, and provide a sound basis for transition from the existing environment to the future. The EA communicates a vision of how the DoD enterprise operates at differing levels of abstraction, by documenting both rules for managing the enterprise and a context within which to apply them:

- Rules: The laws, regulations, policies, strategies, principles, guidance and standards (technical, data, business, mission, etc.) that apply to various parts of the enterprise

- Context: The depictions of relationships (such as hierarchies, processes, information flows, interfaces, syntax, and dependencies) that show how the enterprise guidance applies to each mission and function

Rules enable our distributed organization to function as a single enterprise and move (in unison) toward a common target vision. Context adds clarity and relevance to the rules.

3 An EA Guided Enterprise

Though EA was mandated in law, regulation, and policy to support enterprise IT decisions, DoD has learned that EA can be leveraged to support a vast array of functions ranging from process improvement to organizational restructuring to mission performance enhancement. The Department's approach to applying architecture is to not have an enterprise that's driven by EA,

but rather to use EA to guide the Department's performance improvement strategy – i.e., to help make the operational processes, infrastructure, and materiel solutions of the DoD better. These improvements should also serve to maximize net-centric data sharing and service exposure, discovery and use. The resulting solutions should help achieve improved interoperability, better information sharing, tighter compliance, leaner processes, reduced costs, and more effective mission accomplishment. Developing EA to guide the Department's Performance Improvement relies heavily on three instances of enterprise architecture:

- Strategic Architectures are a set of descriptions focused on the rules and principles that apply to all investments regardless of capability, Component or portfolio. These architectures contain rules and principles that apply to all investments regardless of capability, Component or portfolio. The 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.

- Capability Architectures are set of descriptions focused on portraying the context and rules required to achieve a desired effect through a combination of doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF). The Business Enterprise Architecture (BEA) today is a good example of a collection of capability segment architectures covering Finance, Human Resources, Acquisition, and other business domains.

- Mission Thread Architectures are a set of descriptions focused on describing the process and information flow required to achieve a mission or effect using the full range of required capabilities. A Mission Thread Architecture provides the warfighter's viewpoint by weaving other portions of the DoD Enterprise Architecture together with mission-unique elements. Typically, these architectures focus on process maps that link enterprise capabilities. This is an area that takes full advantage of the intersection between EA-Segments and JCAs.

Each of these types of architecture is essential to the proper functioning of the Department. Working together, they ensure that there is sufficient guidance not only to perform specific capabilities in isolation, but also to ensure that interoperable information flows consistently across capability areas and segments, demonstrating that architected capabilities can be effectively engaged and integrated to achieve the mission objectives of the Department.

4 Using EA to Improve DoD Performance

The strategy for using architectures to guide performance improvement in the Department embodies four key elements:

- Define, develop and maintain (segmented) enterprise architecture. The Department maintains the DoD EA at the DoD Enterprise level and at the Component level, while ensuring that the overarching structure for federating architectures align to DoD's portfolio structure. The DoD architecture is used to ensure that investments are properly assessed in a Federal-wide context by aligning all information technology investments with the Federal Enterprise Architecture (FEA) Reference Models and the Federal Transition Framework (FTF).

- Define, develop and maintain solution architectures. The Department develops and maintains solution architectures for material and non-material initiatives and capabilities that deliver functionality for the DoD information enterprise, ensuring that both the solution architectures and solutions themselves conform with the DoD EA.

- Use DoD architecture information for better-informed decisions. The Department has been using the DoD EA to guide investment portfolio strategies and decisions, define capability and interoperability requirements, establish and enforce standards, guide security and information assurance requirements across the Department of Defense and provide a sound basis for transition from the existing environment to the future. DoD EA is also used to guide solution architectures to clearly articulate requirements, influence design and implementation, and demonstrate interoperability. DoD EA is also being used to review all IT investments, including those related to National Security Systems, for compliance with the DoD EA and applicable approved solution architectures. DoD architecture is used to institutionalize consistent, effective use of architecture across the Department, strengthen the use of architecture in the key decision making processes of the Department, including the Joint Capabilities Integration and Development System (JCIDS), Defense Acquisition System (DAS), Business Capability Lifecycle (BCL), Planning, Programming, Budgeting and Execution (PPBE), Capability Portfolio Management (CPM), and Joint Concept Development and Experimentation (JCD&E), in a manner that enables better-informed decisions.

- Govern the DoD-EA. The Department governs architectures through formal processes consistent with the organizational and functional structure of the Department. Architectures will be registered and approved through the formal governance processes. As part of the governance process, DoD will continue to sustain and apply standards for documenting architecture content to promote reuse, common vocabulary and integration.

5 Applying EA to Improve Governance throughout DoD

The Department conducts periodic assessments of architecture management maturity and the contributions of architecture to mission effectiveness, efficiency, information sharing, and transparency. The Office of the DoD CIO has reorganized the governance structure to better align with emerging policy.

The Architecture and Standards Review Group (ASRG) is the primary governance body responsible for architectures and standards. The ASRG has DoD-wide membership and is responsible for recommending approval of architectures for inclusion in the architecture federation or DoD Enterprise Architecture and approval of IT standards for inclusion in the DISR. The ASRG along with two other review groups, the Enterprise Services Review Group (ESRG) and Information Assurance Enterprise Review Group (IAERG) perform governance functions as part of a larger Enterprise Governance Board (EGB).

5.1 Guidance and Direction Development

One EGB objective is to develop and approve DoD CIO enterprise-wide guidance (including architecture, standards and policies) to determine effectiveness and deficiencies, with resulting courses of action, in satisfying DoD mission needs by:

- Guiding the development of the DoD Enterprise Architecture (DoD EA), related policies and standards.

- Approving enterprise information architectures, policies and standards to guide and support the management of DoD IT within the Planning, Programming, Budgeting, and Execution (PPBE) (including Capability Portfolio Management [CPM] and Capital Planning and Investment Control [CPIC]), Joint Capabilities Integration and Development System (JCIDS) and Defense Acquisition System (DAS) processes.

- Approving enterprise-wide guidance and tool requirements to support the analysis and management of IT across the Department by Component CIOs, Component Acquisition Executives (CAEs), IT Portfolio Management (IT PfM) Mission Area Leads and DoD CPM Co-Leads.

- Tasking tiger teams to research specific issues related to enterprise architecture and IT implementation strategies in a collaborative, transparent and objective manner. Use tiger team reports to help frame enterprise guidance.

- Assessing the technical, operational and financial cost and benefits of potential enterprise services, providing a process by which potential enterprise services can be reviewed and approved for designation as Mandatory Core DoD Enterprise Services and/or Shared DoD Enterprise Services.

5.2 Using EA to Drive Implementation

Another EGB objective is to drive implementation of, and ensure compliance of all IT investments with DoD EA related policies and standards by:

- Tasking Components to develop implementation plans for Mandatory Core Designated DoD Enterprise Services and Shared Designated DoD Enterprise Services, and conduct follow-up reviews on an annual basis to ensure Components comply with their own implementation plans.

- Validating and modifying the review and waiver processes as required to ensure compliance of all IT with applicable portions of the DoD EA.

- Convening as the DoD CIO Investment Review Board (IRB) to review, approve, and oversee the planning, design, acquisition, deployment, operation, maintenance, and modernization of defense business systems the primary purpose of which is to support information technology infrastructure or information assurance activities, and as directed by the Secretary of Defense.

Another aspect of the DoD IT governance process is portfolio management which includes the IT investment prioritization process. The DoD Components are responsible for funding the IT initiatives supporting their respective portions of collaborative, joint programs. Therefore, the portfolio management process must be coordinated in a Department-wide effort in order to focus on the mission of the Department – i.e., Warfighting.

6 Portfolio-based Investment Management Progress

Since 2005, a Four Mission Area construct (i.e., Warfighting, Business, Intelligence, and Enterprise Information Environment) had been used as an IT portfolio management and EA construct in accordance with DoD Directive 8115.01 (IT Portfolio Management). Those designations were purposefully broad to provide a base level of alignment and accountability for managing the Department's IT portfolio. As portfolio management became more valued over time, the DoD moved toward managing all of its investments—not just IT— via portfolios. Whereas the Quadrennial Defense Review of 2005 initiated the Capability Portfolio Management (CPM) process with pilots, the recently signed Capability Portfolio Management Directive (DoD Directive 7045.01) prescribes a structure whereby all DoD programs are to be managed in a suite of portfolios. The content of the overall portfolios continues to evolve, the idea that all DoD investments will be managed as portfolios is established.

The DoD Chief Information Officer (CIO) is now aligning IT Portfolio management as part of the Department's overall portfolio processes – not as a separate, discrete process. In today's world it is impossible to separate core processes from the information flows that support them. Thus, it is logical that IT Portfolio Management (PfM) be a portion of the overall PfM

responsibilities of process owners and organizations across the Department. Consequently, within DoD it is the responsibility of the core process owners and Components to develop architectural content to support their respective areas. The DoD CIO is realigning IT PfM and EA policy with this position. DoD CIO involvement is focused on:

- Providing frameworks as tools to support DoD EA development and use to support IT PfM

- Participating in portfolio management activities across DoD.

Within the CPM construct described above, Segment Architectures as defined by OMB are equivalent in the DoD EA to Capability Architectures -- sets of descriptions focused on portraying the context and rules required to achieve a desired effect through a combination of doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF). Capability architectures (enable the Department to inform and guide IT investments, identify potential gaps and overlaps and understand the broader operational constructs and segment interrelationships. The Business Enterprise Architecture (BEA) today is a good example of a capability architecture that spans multiple segments including Financial Management, Human Resources Management, Acquisition, and others.

7 DoD EA Segment

In response to the evolution of DoD's portfolio management and EA efforts, we have identified a more granular set of EA segments (see Table 1 above). Further, these EA segments are aligned with the JCA overarching Departmental portfolio management construct. As the Department's portfolio management construct matures, the identification of additional EA segments is expected to evolve over time and be incorporated into that construct.

While the DoD EA spans both the DoD Enterprise level and the Component level, the segment architectures exist primarily at the DoD Enterprise level – thereby providing consistent guidance that applies to all programs, initiatives and capabilities within the Department of Defense. Component architectures extend the enterprise-level guidance, providing additional component-specific information that applies to all solutions within their organization. As Enterprise segments solidify, component architectures will begin to align to them specifically (as is already the case where component EAs align with the BEA).

8 Transition Planning in the DoD

The Secretary of Defense sets the strategy, provides oversight, and manages capability integration across all DoD Components. Recognizing that each Component has its own way of doing business, its own constituencies and its own appropriations, it is essential that Components

maintain responsibility for executing their assigned missions, conducting joint operations and ensuring information flows freely across the enterprise.

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 tiers of the Department – DoD Enterprise, Component, and Program. Federation ensures decision makers and implementers understand and align programs and capabilities across tiers. A federated approach allows each tier (in accordance with its Title authority) to leverage the decisions and services of other tiers. Each tier governs the area for which it is responsible, and should acknowledge and maintain consistency with the guidance from higher tiers. To improve understanding across all tiers, DoD enterprise-level architectures depict department-wide rules and constraints while Component-level architectures depict mission-specific services and capabilities and program-level architectures depict solutions that conform to higher tier rules and constraints.

8.1 How the DoD EA Guides Transition Planning

At the Enterprise level, DoD's Federated EA is a set of architectures depicting slices of capability and function that provide guidance to decision makers regarding:

- "What we must do" – a common set of principles, rules, constraints, and best practices that must be followed to meet enterprise goals.

- "How we must operate" – the operational context of the aforementioned principles, rules, constraints, and best practices.

- "When we will transition" - a roadmap (a transition plan) with priorities and strategies for achieving them, as well as milestones, metrics, and resources needed to execute the strategies.

DoD enterprise level architectures typically do not provide implementation guidance or design details for individual systems or solutions, and are not a substitute for management decisions. They inform enterprise-wide decisions, and portray the results. Transition planning adheres to the Department's tiered accountability principle; it is done at the mission, business and enterprise services layers of the Target DoD EA.

8.2 Transition Planning for Core Mission Segments of the Target DoD EA

The Joint Staff is the primary organization for the Department's warfighting mission. The Joint Staff has developed and implemented the JCIDS process as its primary means of prioritizing and managing investments, including IT and National Security Systems. The JCIDS process is driven by strategic direction, input from the Combatant Commanders (COCOMs) in the form of Integrated Priority Lists (IPLs), and the Joint Requirements Oversight Council (JROC) by way of Joint Requirements Oversight Council Memorandums (JROCMs).

8.3 Transition Planning for the Business Services Segments of the Target DoD EA

The Business Transformation Agency's Enterprise Transition Plan (BTA ETP) is the Department of Defense's integrated business transformation plan, which incorporates the transition plans of the Military Services, Components and the DoD Enterprise. It provides a roadmap for achieving DoD's business transformation by implementing changes to technology, process, and governance. It is the conceptual roadmap that implements the DoD business enterprise architecture. It defines the path to a transformed DoD enterprise and identifies business investments that provide enterprise capabilities to support the warfighter and decision makers. The BTA ETP contains time-phased milestones, performance metrics, and a statement of resource needs for new and existing systems that are part of the Business Enterprise Architecture (BEA) and Component architectures. The BTA ETP also includes a termination schedule for legacy systems that will be replaced by systems in the target environment. The BTA ETP provides the context and perspective for understanding the Department's transformation progress. The BTA ETP includes: (a) the acquisition strategy for new systems that make up the target EA, (b) a listing of business legacy systems not expected to be in the target environment, (c) a list of the legacy systems expected to be part of the target environment, and (d) time-phased milestones, performance metrics and a statement of resource needs. Updated annually, the BTA ETP is an integrated product that is used in conjunction with the Report on Defense Business Operations and the BEA. Together they provide important information to DoD leaders to help them evaluate progress, gaps and overlaps between current programs so they can redirect efforts to provide needed business capabilities.

8.4 Transition Planning for the Enterprise Services Segments of the Target DoD EA

8.4.1 DoD IEA

During the development of the DoD IEA, five priorities were identified as areas where increased attention and investment would drive important progress towards achieving net-centric information sharing. These priorities are neither organizations nor functions – they are a way to focus effort across functional areas to achieve goals. Priorities help transform the enterprise by focusing on key needs that will help achieve the target state. These priorities are the fundamental organizational construct for DoD IEA, and focus the architecture on aligning investments with net-centric principles. The following five DoD IEA Priorities have been defined:

- **Data and Services Deployment -** 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** - 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** - 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.

- **Communications Readiness** - 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** - 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.

The DoD IEA enables decision-makers to have informed discussions on key issues driving evolution of DoD's information environment. The DoD IEA empowers 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.

Transformation will be realized over time, as services that are consistent with the Department's net-centric vision are provided and current limiting factors are overcome, enabling increased information sharing. As the principles and rules outlined in DoD IEA are embedded in decision processes across the Department and applied appropriately to DoD investments, they will accelerate the evolution to net-centric information sharing. By reflecting existing DoD CIO-related guidance, policy, and frameworks in a more cohesive vision and informing decision makers across the Department, the DoD IEA plays a key role in transforming the DoD to net-centric operations.

8.4.2 DoD Information Enterprise Strategic Plan and Roadmap
The DoD Information Enterprise (IE) Strategic Plan and Roadmap (SP&R) defines the steps for achieving the DoD Information Enterprise envisioned by the National Military Strategy, QDR, DoD IE Strategic Plan¸ and DoD IEA. It provides a prioritization plan to guide the transformation of the Department from a stove-piped information approach to achieving the Department's net-centric information sharing vision. The SP&R will foster alignment of the Department's net-centric information sharing efforts by identifying, relating and measuring the

development and implementation of specific policies, programs, and initiatives that enable the Department's transition to more fully realizing net-centric effects. The Strategic Plan and Roadmap establishes a baseline for measuring the Department's performance in achieving the goals and objectives of the DoD Information Management/Information Technology (IM/IT) Strategic Plan and the priorities of the DoD IEA. The plan also highlights how organizations are leveraging net-centric information sharing capabilities to improve the effectiveness and efficiency of processes across the Department.

The DoD IE Strategic Plan provides a common understanding of the DoD's shared vision, mission, and governing principles for the IE. The plan identifies six broad goals with associated objectives to "Lead the DoD enterprise to achieve an information advantage for our people and mission partners." **Goal 1** represents the overall goal of the DoD IE Strategic Plan, and the change management in particular that is a major cross-cutting enabler for achieving all the DoD IEA priorities. DoD IE Strategic Plan **Goal 2** aligns with the DoD IEA's DSD priority; **Goal 3** aligns with the Communications Readiness, Computing Infrastructure Readiness, and Netops Agility; **Goal 4** aligns with the SA priority. **Goals 5** and **6**, dealing with Portfolio Management and IT Workforce Development, are cross-cutting enablers of the DoD IEA.

9 Tools for Developing, Implementing, and Managing the DoD EA

Development, implementation, and management of the DoD EA is accomplished through a robust set of tools. Many of these tools have been mentioned earlier in this document. They include the DoD Architecture Framework (DoDAF), DoD Architecture Registry System (DARS), and DoD Information Technology Standards Registry (DISR), and DoD Information Technology Portfolio Registry (DITPR).

9.1 DoD Architecture Framework (DoDAF)

The Department of Defense Architecture Framework (DoDAF) serves as the overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate the ability of Department of Defense (DoD) managers at all levels to make key decisions more effectively through organized information sharing across the Department, Joint Capability Areas (JCAs), Mission, Component, and Program boundaries. It is the Department's means for standardizing representation of architecture information. The DoDAF serves as one of the principal pillars supporting the DoD Chief Information Officer (CIO) in his responsibilities for development and maintenance of architectures required under the Clinger-Cohen Act. It also reflects guidance from the Office of Management and Budget (OMB) Circular A-130, and other Departmental directives and instructions. The current version, DoDAF V2.0 focuses on architectural data, rather than on developing individual products as described in previous versions. In general, data can be collected, organized, and stored by a wide range of architecture tools developed by commercial sources.

9.2 DoD Architecture Registry System (DARS)

The DoD Architecture Registry System (DARS) is the DoD's means to register and catalog all DoD architectures to provide architecture discoverability and accessibility across the Department. It provides a visualization of the federated DoD EA and a means to federate and link architectures to enterprise reference models and segment architectures.

9.3 DoD Information Technology Standards Registry (DISR)

The DoD IT Standards and Profile Registry (DISR) is an online repository of IT standards formerly captured in the Joint Technical Architecture (JTA), Version 6.0. DISR online supports the continuing evolution of the DISR and the automation of all its processes; it can be accessed at https://disronline.csd.disa.mil/a/. DISR online is the repository for information related to DOD IT and National Security Systems (NSS) standards. DISR standards are to be used within DoD as the "building codes" for all new systems. The standards are intended to facilitate interoperability and integration of systems within the Global Information Grid (GIG). DISR also provides the ability to specify profiles of standards that programs will use to deliver net-centric capabilities.

10 Way Ahead for the DoD EA

The DoD EA continues to evolve to ensure it meets the future needs of the Department and provides forward looking guidance. This evolution occurs as DoD EA References are updated, new architectures are developed, and existing architectures are refined. Efforts currently underway that will move the DoD EA forward include the Federation Strategy update, refinement of the ASRG Governance process, development of the Information Enterprise Objective Architecture (IEOA), and establishing Enterprise-wide Reference Architecture as a means to convey guidance,.

10.1 Federation Strategy Update

The GIG Federation Strategy, dated August 2007, is the current federation strategy. It describes architecture description federation as a two step process that includes registration of approved architecture description metadata and alignment of architectures based on activities without regard to the level of the architecture. This strategy is being revised and updated as the DoD Architecture Federation Strategy. We learned that the federation strategy needed to address federation of architecture from two different perspectives, strategic and operational. Based on this, the DoD Architecture Federation Strategy will provide comprehensive descriptions of federation for strategic-level support and operational-level support.

10.2 ASRG Governance Process Refinement

The ASRG Governance process including the sub-working groups with Department-wide representation has been in effect since December 2009. During the course of numerous ASRG and sub-working group sessions, multiple issues have arisen and many lessons have been

learned. Issues resolutions and the lessons learned are the basis for refining the ASRG Governance process. A draft version of the ASRG and sub-working groups' process has streamlined the process and more clearly describes the steps and decision points in the process.

10.3 Development of the IEOA

The DoD IEA describes the principles, rules, and activities for developing, managing, and using the IE. It does not describe the big picture of the objective DoD IE needed to provide context for existing DoD IEA content and for measuring progress in achieving the DoD IE vision. The IEOA will describe the big picture of the objective DoD IE. It will describe the IE capabilities required to support and enable DoD Operations and to achieve the IE vision. The description of capabilities will include the mechanisms needed to provide the capability and the measures for determining progress in achieving the capabilities. The IEOA will be the foundation for establishing priorities for RA development; sequencing roadmap phases; aligning initiatives, projects, and programs; prioritizing investments; and measuring progress in achieving the IE vision. We expect to expand the DoD IEA by merging the content of the IEOA with the DoD IEA so a single document contains a complete and comprehensive description of the DoD IE.

10.4 Enterprise-wide Reference Architecture

DoD has established Enterprise-wide Reference Architecture (RA) as a means to quickly develop and provide Department-wide guidance for a specific subject area. An RA Description document describing the intended use and five elements of an Enterprise-wide RA has been approved and posted. Enterprise-wide RAs may provide guidance in the form of strategic context, principles/rules, patterns, and technical positions. These RAs can be designated from the top as described in the IEOA section or they can be adopted as best practices from existing component RAs.

11 Ongoing Architecture-Based Efforts

There are several ongoing architecture-based efforts that play a role or will play a role in shaping the DoD EA with additional guidance and information to guide and constrain IT investments and solutions. These efforts include the IT Consolidation Strategy and Roadmap (ITCSR), Enterprise-wide Access to Networks and Collaboration Services (EANCS) Reference Architecture (RA), IT Infrastructure Optimization Reference Architecture (ITIORA), and Active Directory Optimization Reference Architecture (ADORA).

11.1 IT Consolidation Strategy and Roadmap (ITCSR)

In August 2010, the Secretary of Defense (SecDef) announced a Department-wide Efficiencies Initiative to move America's defense institutions towards a "more efficient, effective, and cost-conscious way of doing business."[1] DoD Components were directed to conduct a "zero-based

---

[1] Gates, Robert M., (2010). *Statement on Department Efficiencies* Initiative. Accessed from: http://www.defense.gov/speeches/speech.aspx?speechid=1496

review" of how they carry out their missions and priorities and to rebalance resources to better align with DoD's most critical challenges and priorities. As part of the announcement, the SecDef directed the consolidation of IT infrastructure assets to achieve savings in acquisition, sustainment, and manpower costs and to improve DoD's ability to execute its missions while defending its networks against growing cyber threats. The resulting course of action was to consolidate IT assets to optimize the Joint environment and to pursue the consolidation in a way that does not preclude future consolidation at the DoD enterprise level. The high-level, strategic plan for describing the approved course of action is now under development and is titled, "DoD IT Consolidation Strategy and Roadmap" (ITCSR).

Architecture will play a key role in the implementation of the DoD ITCSR by describing the desired future (to-be) state in terms of networks and transport, computing services, end-user device services, and shared enterprise services. The DoD IT Consolidation Goals are focused on improving network security, operational effectiveness, and fiscal efficiency. Influenced by the DoD EA, the DoD will employ a "tiered accountability/ modest federation" approach to IT Consolidation. Under this approach, responsibility and accountability for implementing IT Consolidation initiatives are assigned to different levels in the organization. For example, the DoD CIO is responsible for developing the enterprise IT policy and architectures (i.e., DoD-wide policies, capabilities, standards, reference architectures and rules) and the associated enterprise IT Consolidation Strategy and Roadmap. Each component is responsible for producing a component-level architecture and IT Consolidation plan associated with its own tiers of responsibility in a manner that is aligned with (i.e., does not violate) the enterprise IT policies and architecture. Similarly, program managers are responsible for developing program-level architectures and consolidation plans and for ensuring alignment with the architectures and plans above them. This structure will allow for flexibility while also ensuring linkages and alignment from the program level through the component level to the enterprise level.

11.2 Enterprise-wide Access to Networks and Collaboration Services (EANCS) Reference Architecture (RA)

The EANCS RA was developed in partnership with many DoD organizations to provide Department level guidance for implementing enterprise-wide access to networks and collaboration services capabilities (e.g., Global Authentication and Access Control). The EANCS RA is approved by the DoD CIO for use and conformance across the Department. The purpose of the EANCS RA is to describe the capability to access collaboration services in support of secure information sharing across the Department. It provides architectural patterns to guide, standardize, and enable the most rapid and cost-effective implementation of global authentication, authorization and access control capabilities.

11.3 IT Infrastructure Optimization Reference Architecture (ITIORA)

The Information Technology Infrastructure Optimization Reference Architecture (ITIORA) was developed with the intent of standardizing the delivery of Information Technology (IT) Infrastructure

Services across the Department of Defense (DoD). In order to achieve this goal, the ITIORA provides guidance on optimizing DoD IT infrastructure by taking a service delivery-based approach to identifying a common set of IT infrastructure services and their optimal level of service delivery. In doing so, the ITIORA forms a framework for consolidation upon which the DoD can develop further initiatives to optimize and standardize the DoD IT Infrastructure. The ITIORA is currently in the EGB/ASRG governance process.

11.4 Active Directory Optimization Reference Architecture (ADORA)

ADORA is intended to guide and inform DoD Enterprise and CC/S/A efforts to optimize existing AD environments toward the goal of a single logical, seamless and secure DoD Information Environment in a visible, accessible, understandable and trusted manner. The ADORA will be a primary source of guidance for the development of more detailed solution CC/S/A architectures and associated engineering and technical artifacts. The ADORA seeks to optimize the structure of the DoD AD environment and enhance the way AD is used in DoD to make authentication and access decisions. The AD optimization end-state described in the ADORA eliminates the stove pipes created by today's AD footprint and focuses on delivering enhanced capability to the Warfighter through increased collaboration and information portability. Improving the ability to securely share information and communicate across AD forests is an important step toward the vision of a single, seamless DoD Information Environment. The ADORA is currently in the EGB/ASRG governance process.

12 Key Artifacts Associated with the DoD EA

The DoD Enterprise Architecture (DoD EA) is a federation of architectures. These architectures are developed and maintained at the Department, capability area, and Component levels. The associated DoD Architecture Strategy (found at https://www.intelink.gov/wiki/DoD_AS) describes these concepts. A wiki version of the DoD Enterprise Architecture (https://www.intelink.gov/wiki/DoD_CIO/DoD_EA) provides the latest DoD EA-related information as well as a context for the architecture-related information that is also shown in the tables below[2]. **Table 2** contains links to additional key information about the DoD EA and associated Enterprise Architecture descriptions.

Table 2 - Key Information about the DoD Enterprise Architecture

Span	Artifact Name	Artifact Location
DoD EA Guidance and Tools	DoD Architecture Registry System (DARS)	https://dars1.army.mil/IER2/
	DoD Information Technology Portfolio Repository (DITPR)	https://ditpr.dod.mil/

---

[2] Some URLs have specific additional requirements for accessing the documents.

Span	Artifact Name	Artifact Location
	DoD Information Technology Standards Registry (DISR)	https://disronline.csd.disa.mil/a/
	DoD Architecture Framework (DoDAF)	http://cio-nii.defense.gov/sites/dodaf20
Business	Business Enterprise Architecture (BEA)	http://www.bta.mil/products/bea.html
	Business Enterprise Transition Plan (Business ETP)	http://www.bta.mil/products/ETP.html
	March Congressional Report on Defense Business Operations	http://www.bta.mil/products/Congressional.html
Warfighting	WMA IT Portfolio Management Implementation Plan, dated 18 July 2008	**On SIPRNet**: http://intelink.sgov.gov/w/images/3/34/WMA_ETP_July_2008 **(update work underway)**
Information	Defense Information Enterprise Architecture (DIEA) v 1.1	http://www.defenselink.mil/cio-nii/sites/diea/
	DoD Information Enterprise Strategic Plan and Roadmap (SP&R)	https://www.intelink.gov/wiki/Portal:DoD_IE_Strategic_Plan_and_Roadmap
	DoD IM/IT Strategic Plan	https://www.intelink.gov/wiki/DoD_CIO/DoD_IESPR/StratPlan
	DoD Information Sharing Implementation Plan April 2009	http://www.defenselink.mil/cio-nii/docs/DoD%20ISIP%20-%20APR%202009_approved.pdf
	GIG 2.0 Documents	https://www.intelink.gov/wiki/Global_Information_Grid_2.0
Air Force	Air Force Strategic Plan	http://www.safxc.af.mil/shared/media/document/AFD-080214-046.pdf
Department of Navy	DON Enterprise Architecture (EA)	https://www.intelink.gov/wiki/DONEA#Officially_Released_Versions_of_DON_Enterprise_Architecture
	DON IM&IT Strategic Plan, FY2008-2009	http://www.doncio.navy.mil/Products.aspx?ID=788

Span	Artifact Name	Artifact Location
	DON Enterprise Architecture (EA) Strategy, 18 February 2009	http://www.doncio.navy.mil/PolicyView.aspx?ID=904
	DON Campaign Plan	http://www.doncio.navy.mil/Products.aspx?ID=1356
Defense Information Systems Agency (DISA)	GIG Convergence Master Plan	https://www.intelink.gov/wiki/DGCMP
Defense Logistics Agency (DLA)	DLA Strategic Plan FY07 - FY13	http://www.dla.mil/library/stratplanfeb2007.pdf
U.S. Transportation Command (USTRANSCOM)	Joint Deployment and Distribution Architecture-Enhanced (JDDA-E)	https://www.intelink.gov/wiki/JDDA-E
	U.S. Transportation Command Strategic Plan	http://www.transcom.mil/dpo/ **(Click current year Strategic Plan at top of page)**

Date: _/ MARCH 11_

Brian G. Wilczynski, SES
Director, Architecture & Infrastructure
ASD(NII)/DoD CIO

Date: _3/1/11_

Lloyd Thrower
Director, Strategic Plans & Investment Management
ASD(NII)/DoD CIO