

Department of Defense Information Enterprise Architecture Version 1.1



May 2009

**Prepared by:
Department of Defense
Office of the Chief Information Officer**

(This page intentionally left blank)

EXECUTIVE SUMMARY

The Department of Defense (DoD) Information Enterprise Architecture (IEA) provides a common foundation to support accelerated Department of Defense (DoD) transformation to net-centric operations and establishes priorities to address critical barriers to its realization. The DoD Information Enterprise (IE) comprises the information, information resources, assets, and processes required to achieve an information advantage and share information across the Department and with mission partners. The DoD IEA describes the integrated DoD IE and the rules for the information assets and resources that enable it.

DoD IEA 1.1 unifies the concepts embedded in the Department's net-centric strategies into a common vision, providing relevance and context to existing policy. DoD IEA 1.1 highlights the key principles, rules, constraints and best practices drawn from collective policy to which applicable DoD programs, regardless of Component or portfolio, must adhere in order to enable agile, collaborative net-centric operations. 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.

Core principles and rules (summarized in Appendix A) are organized around five key priorities where increased attention and investment will bring the most immediate progress towards realizing net-centric goals:

- Data and Services Deployment (DSD)
- Secured Availability (SA)
- Computing Infrastructure Readiness (CIR)
- Communications Readiness (CR)
- NetOps Agility (NOA)

DoD IEA 1.1 enables DoD decision-makers to have informed discussions on key issues driving evolution of DoD's information environment. DoD IEA 1.1 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 1.1 to strategically align their programs and architectures with the enterprise net-centric vision. DoD IEA 1.1 addresses a "To Be" vision 3-5 years in the future, and will influence the Program Objective Memorandum process.

Transformation will be realized over time, as services 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 1.1 are embedded in decision processes across DoD and applied appropriately to DoD investments, they will accelerate the Department's evolution to net-centric information sharing. The Department's biggest challenge ahead is not deciding what will be in the next DoD IEA release, but rather how to institutionalize the principles and rules established in this one. By reflecting existing DoD CIO-related guidance, policy, and frameworks in a more cohesive vision and informing decision makers across the Department, DoD IEA 1.1 will play a key role in transforming the DoD IE to net-centric operations.

(This page intentionally left blank)

TABLE OF CONTENTS

Introduction	1
Transformation Context.....	3
Tiered Accountability and Federation	3
DoD Enterprise Architectures: Purpose and Scope.....	3
DoD IEA 1.1 Overview	5
Principles, Rules and Priorities	5
Using and Applying Principles and Business Rules	7
DoD Information Enterprise Priorities	8
Data and Services Deployment (DSD).....	8
Enabling the Data and Services Environment	8
Enterprise Services	9
Principles and Business Rules	10
Secured Availability (SA)	12
Enabling Net-Centric Secured Availability	12
Maintaining Security in an Ever Changing Environment	13
Principles and Business Rules	14
Shared Infrastructure Environment	15
Principles and Business Rules	16
Computing Infrastructure Readiness (CIR).....	17
Delivering Net-Centric Computing Infrastructure	17
Standardizing GIG Computing Infrastructure Nodes	18
Principles and Business Rules	20
Communications Readiness (CR)	21
Enabling Communications Readiness Environment	21
Principles and Business Rules	22
NetOps Agility (NOA)	23
Enabling NetOps Agility	24
Principles and Business Rules	24
DoD IEA 1.1 Products.....	26
DoD IEA Evolution.....	26
The Challenge Forward	27
Appendix A: DoD IEA Principles and Business Rules.....	A-1
Appendix B: DoD IEA Hierarchical Activity Model.....	B-1
Appendix C: Acronyms	C-1
Appendix D: Applying the DoD Information Enterprise Architecture (DoD IEA)	D-1
Appendix E: Compliance with the DoD Information Enterprise Architecture (DoD IEA) ...	E-1
Appendix F: Mapping DoD IEA Activities to NCOW RM Activities	F-1
Appendix G: Glossary	G-1

(This page intentionally left blank)

Introduction

The Department of Defense Information Enterprise Architecture version 1.1 (DoD IEA 1.1) provides a common foundation to support accelerated transformation of the Department of Defense (DoD) to net-centric operations. It presents the vision for net-centric operations and establishes near-term priorities to address critical barriers that must be overcome to achieve that vision.

The DoD Information Enterprise (IE) comprises the information, information resources, assets, and processes required to achieve an information advantage and share information across the Department and with mission partners. As such, the DoD IEA defines the layer of services and standards that enable Information Management (IM) operations and drive the fundamental concepts of net-centricity across all missions of the Department.

DoD Net-Centric Vision:

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.
- An available and protected network infrastructure (the GIG) that enables responsive information-centric operations using dynamic and interoperable communications and computing capabilities.

Each Component and portfolio within the DoD is tasked with implementing net-centricity while ensuring compliance of IT investments with the full range of DoD IE management policy and guidance, including (among others):

- *DoD Net-Centric Data Strategy* (May 2003)
- *Data Sharing in a Net-Centric DoD* (DoDD 8320.02, December 2004)
- *Guidance for Implementing Net-Centric Data Sharing* (DoD 8320.02-G, April 2006)
- *DoD Net-Centric Services Strategy* (May 2007)
- *DoD Information Sharing Strategy* (May 2007)
- *DoD Information Assurance Policies* (DoDD 8500.01E, October 2002)
- *DoD Computing Infrastructure Strategy* (September 2007)
- *DoD Telecommunications Policies* (DoDD 4640.13 and DoDD 4650.1, November 2003 and June 2004, respectively)
- *DoD NetOps Strategy* (February 2008)

DoD programs providing IT capabilities must also adhere to applicable DoD CIO established global standards such as the Universal Core information exchange schema and use, where appropriate, Core Enterprise Services provided through the Net-Centric Core Enterprise Services (NCES) program. Additionally, DoD IT leverages the shared common computing and communications infrastructure of the Global Information Grid (GIG). Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not and will not be connected to the enterprise network.

The DoD IEA focuses policy and guidance towards the common vision, enhancing the ability of decision makers to assess investment opportunities against the vision of net-centric operations. The DoD IEA 1.1 unifies the concepts embedded in the Department's net-centric strategies into a common vision, providing relevance and context to all existing policies, guidance, architectures and frameworks within the Department today. The key principles, rules, constraints and best practices drawn from DoD policy and guidance apply to programs delivering IT capabilities within the Department, regardless of Component or portfolio, must adhere in order to ensure compliance with the net-centric vision, and enable agile, collaborative net-centric information sharing.

DoD IEA 1.1 does not replace the underlying policies, standards or frameworks. By tying together existing Departmental guidance, policy and frameworks into a single vision and empowering investment decision makers across all DoD Components and portfolios, DoD IEA 1.1 will directly impact decision making across DoD.

DoD IEA 1.1 will enable decision-makers to have informed discussions on the key issues driving the evolution of DoD's net-centric environment.

Each rule is linked to an underlying policy and/or corresponding standard through the associated activity model. The DoD IEA will enable decision makers across the Department to have informed discussions on key issues driving the evolution of DoD's net-centric information environment.

By focusing on the "To Be" vision 3-5 years in the future, the DoD IEA 1.1 is positioned as a tool to be used by DoD investment decision makers to inform enterprise-wide net-centric transformation and portfolio management investments as part of the Program Objective Memorandum process decisions, and by Components to strategically align their programs and architectures with the enterprise net-centric vision.

Transformation Context

Tiered Accountability and Federation

The Secretary of Defense sets the strategy, provides oversight, and manages capability integration across all DoD Components (hereafter, simply 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 Department, Capability Portfolios, Components, and Solutions. *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. 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.

DoD Enterprise Architectures: Purpose and Scope

The DoD's Federated Enterprise Architecture is a set of enterprise (Department, Capability, and Component) 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 architectures typically will not provide implementation guidance or design details for individual systems/solutions, and are not a substitute for management decisions; they simply inform enterprise-wide decisions and portray the results.

Enterprise Architecture Primary Purpose - to inform, guide, and constrain the decisions for an enterprise, **especially those related to Information Technology investments.**

*A Practical Guide to Federal
Enterprise Architecture, Version 1.0
Chief Information Officer Council*

Enterprise architectures focus on three sets of customers:

1. 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.
2. IT architects across capability portfolios, Federal Agencies and DoD Components. They use the architectures to align touchpoints and boundaries as well as to identify interoperability gaps and the requirements for federation. The DoD federated set of architectures is collectively known as the federated DoD Enterprise Architecture (DoD EA). The DoD EA is in turn federated with the Federal Enterprise Architecture (FEA) and other external architectures.
3. DoD and Component Program Executive Officers (PEOs), Program Managers (PMs) and their corresponding functional requirements managers. Enterprise architectures provide these customers with design principles by enabling each program to filter applicable laws, regulations, policies, standards and frameworks imposed from internal and external sources.

Enterprise architectures present a “To Be” vision intended to influence how future systems are designed and built. They do not affect existing, deployed systems, except to the extent that they receive investment dollars for modernization. In other words, enterprise architectures do not require a forced retrofitting of existing systems, services, or capabilities.

While the DoD IEA guides the implementation of solutions that make information more accessible, decisions as to who has access to specific information elements remain within the Department’s leadership and command structure.

DoD IEA 1.1 Overview

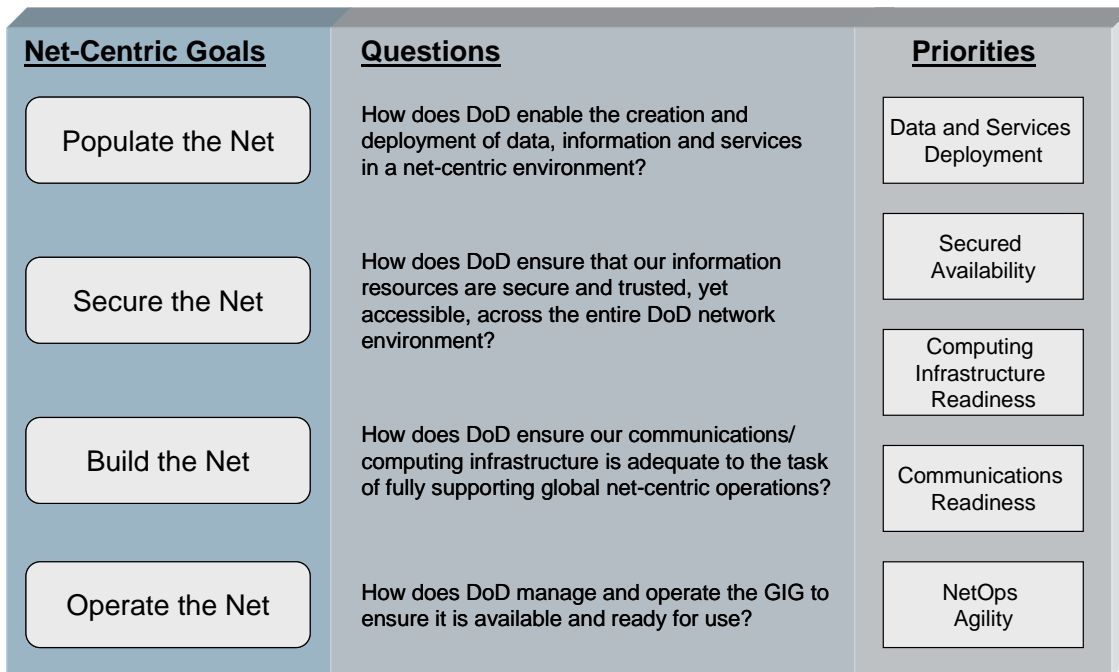
Principles, Rules and Priorities

The DoD IEA 1.1 establishes a very limited set of core principles and rules drawn from collective DoD IM policy and guidance, and presents them as a set of basic criteria for all applicable IT investments. These guidelines will drive net-centric information sharing, increasing effectiveness, efficiency, and interoperability across the Department. Several principles are universal, cutting across all capability areas, and should be considered and applied appropriately to all other IT decisions. These are presented below:

Defense Information Enterprise Global Principles

- DoD CIO-governed resources are conceived, designed, operated and managed to address the mission needs of the Department.
- Interoperability of solutions across the Department is a strategic goal. All parts of the 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. DoD achieves infrastructure interoperability through definition and enforcement of standards and interface profiles and implementation guidance.
- Data assets, services, and applications on the GIG shall be visible, accessible, understandable, and trusted to authorized (including unanticipated) users.
- Defense Information Enterprise services shall advertise service-level agreements (SLAs) that document their performance, and shall be operated to meet that agreement.
- 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.

Other principles and rules are better introduced and positioned as they relate to specific DoD IE priorities. 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 neither organizations nor functions – they are a way to focus effort across cross-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 1.1, and focus the architecture on aligning investments with net-centric principles. The following priorities have been defined:

- **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.
- **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.
- **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.

Using and Applying Principles and Business Rules

Principles are enduring guidelines that describe ways in which an organization should fulfill its mission. Principles express an organization's intentions so that design and investment decisions can be made from a common basis of understanding. Business rules are definitive statements that constrain operations to implement the principle and associated policies.

The vision, principles, and rules in the DoD IEA support the DoD's warfighting, 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 1.1 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.

Definition: 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 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 information technology, including national security systems.

DoD Information Enterprise Priorities

Data and Services Deployment (DSD)

Achieving a rich information environment demands a cultural shift regarding how information is considered. Today's data silos support an approach in which information is hidden and hoarded. Meeting the needs of unanticipated users requires information to be visible and shared. The world wherein *information is power* is shifting to a culture that embraces and leverages the *power of information*.

The net-centric vision assumes a rich information sharing environment in which data and services will be widely available, easily discoverable, usable and trusted across the GIG. Sufficient context will be available to understand the data and services that are available and to determine suitability for a particular purpose. All data and services that exist will be visible and accessible. As a result, information stovepipes will be eliminated and decision-making agility and speed increased. Regardless of time or place, users will be able to say, "*I can get the information I need to perform my mission.*"

The DSD priority focuses the Department on the challenges of transforming its approach from deployment of systems to the delivery of information and services and provides definitions, rules and principles that will guide us in achieving the net-centric vision.

Enabling the Data and Services Environment

Services and support for information providers and consumers must ensure information in a net-centric environment is secure, properly available and effectively used. Different ways to fund and sustain IT solutions will be required as DoD increasingly seeks shared information, solutions, processes and resources. Near-term issues include:

- **Practicing Service Orientation** – As capabilities are defined, solutions should be made available in the net-centric environment through *services*. Training to foster a common understanding of key Service-Oriented Architecture concepts, such as separation of interfaces from implementations, or separation of business logic from infrastructure functions, will be critical. Additionally, related practices such as the current *DoD Information Assurance Certification and Accreditation Process* will need to be adjusted to facilitate the rapid deployment of new services across an accredited, net-centric infrastructure.
- **Developing Communities of Interest (COIs)** – The COI approach is key to solving high priority data, information and services issues. COIs address information sharing gaps by identifying the most important data and capabilities needed to support agile and collaborative community business processes.
- **Enabling Information Discovery** – The ability to find data and services in the net-centric environment is critical. It must be possible for any user to obtain services from authorized sources. Information must be tagged with metadata at the time of creation, not retroactively. Content discovery brokers must be developed to scan

information/service registries across the GIG to locate requested information content.

- **Formalizing Service Interfaces** – Services must be discoverable, understandable, and usable. That will require information providers to register their services and provide details that will allow consumers to use, manipulate or transform data.
- **Defining Business Models for Service Operations and Sustainment** – Traditional funding strategies in the “stove-pipe” model provide end-to-end solutions for applications, data and underlying hardware. New approaches must be developed that accommodate shared expenses between information providers and consumers.
- **Establishing Enterprise Governance for Common Services** – Increasing the value of data and services and easing the impact on consumers will require common functionality and interfaces for the essential core services. Establishing technical, operational, and programmatic oversight and governance is essential to the emergence of a functioning ecosystem of providers and consumers.

The DoD CIO governed DoD IE enables a new, net-centric way of working – it is constructed from the information itself, as well as a set of standards, services and procedures that enable information to be widely available to authorized users. It is a set of services and tools that provide information and capabilities that enable end-user communities to more effectively and efficiently support mission operations. Finally, the DoD IE includes the networks over which information travels and the security protocols that protect it.

Communities of Interest must decide the specific information their users need to perform their missions. Each community must determine, design and implement solutions based on business process review and engineering efforts that leverage enterprise resources to meet mission needs.

Enterprise Services

As the net-centric environment evolves, an ever increasing number of information services will become available to users across DoD. It will be critical to maintain acceptable and measurable levels of support for all Enterprise capabilities. Users will have certain expectations regarding the pedigree, reliability and availability of Enterprise Services, and these attributes should be consistent across all such services. Being able to do this requires Enterprise Services to be defined and characterized.

An Enterprise Service is any capability provided for broad use across the DoD that enables awareness of, access to or delivers information across the GIG.

- Enterprise Services may be provided by any source within the DoD - or any of its trusted partners.
- Enterprise Services providing data or information shall be authoritative and, thus, trusted as being accurate, complete and having assured integrity. Authoritative information has a pedigree that can be traced to a trusted source.

- Enterprise Services must be hosted in environments that meet minimum GIG computing node standards in terms of availability, support and backup.

A small set of Enterprise Services, designated as Core Enterprise Services, are mandated for DoD-wide use by the DoD CIO in order to provide enterprise-wide awareness, access and delivery of information via the GIG.

Principles and Business Rules

The principles and rules detailed here define how data and services will be treated in the net-centric environment and, thus, apply to all appropriate DoD IT investments regardless of Component or portfolio.

Data & Services Deployment Principles

- Data, services and applications belong to the DoD Enterprise. Information is a strategic asset that must be accessible to the people who need it to make decisions.
- 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.
- Only handle information once (the OHIO principle). Information that exists should be reused rather than recreated.
- 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.
- Data, services and applications must be visible, accessible, understandable, and trusted to include consideration of “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

- Authoritative data assets, services, and applications shall be accessible to all authorized users in the Department of Defense, and accessible except where limited by law, policy, security classification, or operational necessity.
- COIs will determine which data sources are authoritative and will not declare any source authoritative without establishing a valid pedigree.
- All authoritative data producers and capability providers shall describe, advertise, and make their data assets and capabilities available as services on the GIG.
- All authoritative data assets and capabilities shall be advertised in a manner that enables them to be searchable from an enterprise discovery solution.
- Data will be described in accordance with the enterprise standard for discovery metadata (the DoD Discovery Metadata Specification (DDMS)).
- Mission or business functions will be made available to the enterprise as a network-based service with a published, well-defined interface.
- Services shall be advertised by registering with an enterprise service registry.
- COIs should develop semantic vocabularies, taxonomies, and ontologies.
- Semantic vocabularies shall re-use elements of the DoD Intelligence Community (IC)-Universal Core information exchange schema.
- Vocabularies, taxonomies, and ontologies must be registered with the enterprise for visibility, re-use and understandability.
- Existing enterprise data, services, and end-user interfaces shall be used whenever possible, practical and appropriate, instead of re-creating those assets.

Secured Availability (SA)

All DoD activities involve decision making based on information, and as a result, the GIG is and always will be a high priority target. DoD networks and information are constantly threatened by a variety of adversaries, including nation states, terrorist and criminal organizations, insiders and common hackers. The availability, reliability, and resiliency of the GIG are critical to successfully maintaining information superiority and Information Assurance (IA) is a foundational element for addressing each of these concerns.

Delivering on DoD's net-centric vision requires a robust set of IA capabilities. Sharing information throughout the government, as well as with DoD's industry and coalition partners, demands an assured environment. IA provides the users of the net-centric environment with the trust and confidence that the integrity of the information is maintained, that information systems will be there when needed and remain under DoD control, and that adversaries are not able to compromise the decision space. In this context, IA is essential to countering the increased threats brought about by the greater interconnectivity and interdependency in a net-centric environment.

Secured Availability (SA) addresses several challenges the Department faces in achieving a fully net-centric environment. SA protects and secures critical data, capabilities, IT infrastructures and data exchanges while providing authentication and non-repudiation of GIG information and transactions. It also makes it possible to rapidly and securely respond to incidents threatening GIG operations. Throughout DoD's transition to a net-centric environment, additional IA capabilities may be required by a given program to meet the SA rules and principles stated here; however, as IA shifts toward enterprise-wide SA services, such interim programmatic solutions will be replaced.

Enabling Net-Centric Secured Availability

Fully implementing SA in the net-centric environment requires new technologies, new policies and new levels of collaboration within the Department and among its federal, state, local, industry and coalition partners. Successful implementation of capabilities providing Secured Availability will serve all DoD missions and COIs. Key elements include:

- Providing and managing assured identities for all users, services, and devices to facilitate dynamic information sharing within and across the network boundaries of organizations at varying trust levels.
- Permanently and incorruptibly binding metadata to associated data objects (at the time of the object's creation, not retroactively) to facilitate assured data visibility and handling.
- Assessing threats and risks associated with the software, hardware and services supply chain to enable DoD program, security, and operations personnel to understand the level of trust that can be associated with the IT components they acquire, manage or use.

- Enabling rapid modification of access, resource allocation or prioritization (e.g., bandwidth, processing, and storage) through enterprise-wide, policy-based management in response to changing mission needs or threats based on directory-provided attributes for services and users
- Improving ease of management for enterprise-wide security services and infrastructure (e.g., encryption, crypto key management, identity, privilege and security configuration management, and audit).

Maintaining Security in an Ever Changing Environment

The GIG will be a continuing target of attack and the IA community must continue to counter the entire range of threats brought about by the greater interconnectivity and interdependency of DoD systems. Being able to effectively assess the security posture of the constantly changing GIG, evaluate emerging technologies, assess threats, and adjust investment priorities is increasingly critical to DoD's security.

Near-term initiatives emphasize solutions that provide immediate return on investment, while maintaining and expanding current Computer Network Defense (CND) capabilities. To maintain the advantage offered by net-centric operations, the GIG must be designed to "fight through" these attacks and reconstitute critical capabilities during and after these attacks.

Departmental priorities are likely to feature investments that represent incremental progress toward SA implementation in the net-centric environment. Resource commitments are expected to provide increased protection for data in transit and at rest, improve interoperability, accelerate information management and data exchange automation, and increase IA workforce readiness. Lastly, the Department will ensure Mission Assurance concerns are addressed as part of DoD's overall risk assessment framework through policies, standards, processes and initiatives that address hardware, software, and supplier assurance concerns.

Principles and Business Rules

The following principles and rules have been established to guide IT investment decisions and ensure programs properly emphasize implementation of Information Assurance to achieve Secured Availability.

Secured Availability Principle

- 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.

Secured Availability Business Rules

- 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.
- 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.
- 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.
- DoD programs must clearly identify and fund 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.

Secured Availability Principle

- 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.

Secured Availability Business Rule

- GIG assets must establish and implement a Mission Assurance capability that addresses hardware, software and supplier assurance through engineering and vulnerability assessments.

Secured Availability Principle

- 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 Defense Information Enterprise.

Secured Availability Business Rules

- 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.
- 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.
- Metadata containing access control and quality of protection attributes shall be strongly bound to or associated with information assets and utilized for access decisions.

Secured Availability Principle

- Agility and precision are the hallmark of twenty-first 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 Rule

- DoD programs must demonstrate that their network, data assets, services, applications and device settings that control or enable IA functionality have been established, documented and validated through a standard security engineering process.
- 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 Environment

The remaining three priorities – Computing Infrastructure Readiness (CIR), Communications Readiness (CR) and NetOps Agility (NOA) – depict DoD’s shared infrastructure environment. Collectively, they represent the hardware layers of the GIG along with management and operational facilities that enable the Department to dynamically allocate, deploy or redirect infrastructure resources anywhere, anytime, in any operational environment. This may mean dynamically scaling resources allocated to critical applications and services or staging certain information forward to mitigate issues of intermittency in the tactical environment. It could mean rapidly deploying entire networks with a full range of capabilities to support a new theater of operations or recover from a natural or man-made disaster. These challenges require a robust infrastructure, one that is modular, scalable and can securely operate across a wide variety of environments.

Principles and Business Rules

The following core principles and business rules were identified as relevant and applicable to the three priorities representing the GIG’s entire common infrastructure environment (CIR, CR, NOA):

Shared Infrastructure Principles

- 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.
- The GIG shall enable connectivity to all authorized users.
- GIG infrastructure must be scalable, changeable, deployable and manageable rapidly while anticipating the effects of the unexpected user.

Shared Infrastructure Business Rules

- 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.
- 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)

The DoD net-centric vision requires information and services to be visible, accessible, understandable and trusted across the Department. Information is an enterprise asset, decoupled from associated applications, and ready and accessible to meet previously unanticipated needs arising from new circumstances or mission needs. Today's environment is typified by dedicated hardware for specific applications. Information is tied to the application, the location and the operating system. Current Defense Enterprise Computing Centers (DECCs) and equivalent non-government implementations focus on determining capacity and utilization requirements for each individual system or application. This approach can lead to poor utilization of computing resources and require additional hardware and software to be purchased to accommodate dynamic usage and future growth. Contingency planning in this paradigm is accomplished by reserving capacity dedicated to a specific use.

As the Department moves farther down the net-centric operations path, the underlying computing infrastructure for core applications and services must transition towards the delivery as a net-centric capability and not discrete chunks of technology. Net-centric CI will leverage the GIG's distributed computing resources to provide infrastructure that appears to the end-users or applications as one virtual capability. Shared computing and data storage resources will be virtually allocated and the mechanism for doing so will be transparent to users. By "virtualizing" how users view the computing infrastructure, DoD can begin reducing technical and administrative barriers to sharing resources, and provide more agile and scalable support for information sharing across the GIG.

As computing infrastructure evolves to better support net-centric operations, it must take into account the needs of edge users – those at the forward or leading edge of the mission operations environment. The concept of building and maintaining an agile computing environment must support end-users operating in environments challenged by intermittency and low bandwidth.

The CIR priority focuses on the Department's challenges in transforming its legacy of system-specific computing infrastructures to shared GIG computing infrastructure nodes that can deliver guaranteed levels of capability to consumers and providers of the Department's data and services. CIR seeks to transform DoD GIG CI from a hardware- and program-centric infrastructure, to one that is dynamic, shared, adaptable and sufficient to support global net-centric operations.

Delivering Net-Centric Computing Infrastructure

Computing infrastructure in the net-centric environment will be customer-driven, shared, dynamically allocated and automatically monitored and configured. Net-centric computing infrastructure will enable:

- **Location-independent storage** – Services and applications will share storage anywhere across the GIG, allowing consolidation and efficient use of data storage

resources. Likewise, users will be able to access information transparently from anywhere across the GIG.

- **Dynamic, automated storage provisioning** – Experience-derived knowledge and use patterns will be used to heuristically allocate data storage. Thus, CI will be able to “learn” from past usage experience to better serve users.
- **Virtualized application environments** – Applications will be hosted in shared versus dedicated environments, enabling dynamic changes to processor and storage capabilities depending upon usage patterns. Hosting environments provide seamless access to all applications and services regardless of their physical location.
- **Automated status reporting** – All GIG CI resources will continually report their status, thus enabling NetOps to have a continuous view of the status of CI resources across the GIG for situational awareness and command and control monitoring.

Transitioning to this net-centric computing infrastructure will bring many benefits to the Department’s operations:

- **Reduced complexity** - Many of the Department’s existing capabilities have grown through independent acquisitions of components, without an overall vision or architecture in mind. The emerging best practices for large-scale data center operations (including management by SLAs) will drive simpler, more consistent infrastructures.
- **Better responsiveness** – The ability to monitor GIG infrastructure across all applications, services, and user groups, along with the ability to respond dynamically to data storage and processing load will make it easier, faster and less expensive to allocate additional resources to meet new, unanticipated demands.
- **Shared CI Resources** – With the ability to share resources dynamically among applications, services, and user groups, peak transient CI demand for an application or service can be met by prioritization of the CI “pool” and by providing available infrastructure resources dynamically in response to priority uses.
- **Increased consolidation opportunities** – With the ability to share processing and storage, the need to build excess capacity in every individual application’s hardware in order to meet increased or unexpected user demand will be eliminated. This will have a dramatic positive effect on the overall cost of operations.
- **Support to the edge** – The focus on highly available and accessible information resources that scale dynamically to meet user demand and geared to support continuous operations will greatly enhance capabilities available to users at the forward edge of the mission operations environment.

Standardizing GIG Computing Infrastructure Nodes

In the net-centric operating environment, applications and services will no longer be hosted and maintained on dedicated hardware. They will be resourced virtually on GIG Computing Nodes (GCNs) spread across the GIG’s pooled resources. GCNs are IT facilities that provide hosting for applications and services, data storage and content staging in controlled environments that ensure capabilities are delivered within specified service levels. GCNs provide managed physical security, backup and Information Assurance capabilities for all IT services they host. As depicted in the table below,

GCNs may be established at several different scales, ranging from fixed enterprise scale computing centers, to regional or area processing centers, down to local- or unit-level computing centers. Standardizing definitions and rules around GCNs is essential to delivering net-centric computing infrastructure capabilities successfully. GIG CI resources must be brought to the edge via a robust, responsive, and adaptable fixed and deployed GCN taxonomy. All GCNs must be IA / NetOps certified and accredited for adherence to computing service provider (CSP) adequacy criteria.

	Enterprise Computing Infrastructure Node	Regional Computing Infrastructure Node	Modular, Deployable CI Node
Classes	<ul style="list-style-type: none"> • Defense Information Systems Agency (DISA) • Government • DoD Component • Commercial 	<ul style="list-style-type: none"> • Primary Geographic Theater (Europe, Pacific) • Combatant Command (COCOM) 	<ul style="list-style-type: none"> • Maritime, Air, and Ground tactical enclave (Enclave email, content staging, collaboration)
Characteristics	<ul style="list-style-type: none"> • Fixed / permanent resources • High bandwidth Defense Information Systems Network (DISN) Core backbone • Hosts Enterprise net-centric apps and Core Enterprise Services, regional content staging • Enterprise size computing / storage • Scalable based on SLAs, available space and power 	<ul style="list-style-type: none"> • Fixed / permanent resources • High bandwidth DISN Core backbone • Hosts regional applications, regional content staging • Regional scaled computing and storage • Scalable based on SLAs, available space and power 	<ul style="list-style-type: none"> • Mobile / transportable resources • Assembled and deployable based on enclave requirements • Operational and tactical level computing and storage • Scalable based on connection of additional modules

Principles and Business Rules

The principles and rules detailed here should guide the Department in building agile computing infrastructure environments that will support net-centric implementation of IT applications and services, meeting the needs of all to the edge.

Computing Infrastructure Readiness Principles

- 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.
- 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.
- Computing infrastructure must be able to provide secure, dynamic, computing platform-agnostic and location-independent data storage.
- 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

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

Communications Readiness (CR)

The net-centric vision requires a dependable, reliable, ubiquitous network that eliminates stovepipes and responds to dynamic scenarios by bringing power to the edge. To ensure effective information transport, a close relationship must exist between the computing infrastructure, intelligence and network operations priorities to support access to GIG services.

Data transport to all users across multiple security domains presents a challenge in current technology. Seamless access to standardized services from anywhere on the GIG is a primary goal. All data must be available to all authorized users in all places and at all times. Additionally, the ability to rapidly deploy, expand or redeploy infrastructure elements is essential. Recovery of systems from damage or failure is necessary to provide GIG access in mission critical situations. Thus, reliability, maintainability and availability are elements that require significant focus. Interoperability between systems and technologies is also paramount to seamless access.

The CR priority focuses on the communications infrastructure and supporting processes that ensure information transport is available for all users (both fixed and mobile) across the GIG. This infrastructure includes physical networks, protocols, waveforms, transmission systems, facilities, associated spectrum management capabilities and other assets that provide: 1) wireless line-of-sight, 2) SATCOM and other beyond-line-of-sight, 3) fiber optic and traditional wireline, and all other physical transmission media. The priority is built on a core foundation of transport elements, with the advancement of technology, which will support the full scope of network convergence for voice, data, and video across multiple security levels.

Enabling Communications Readiness Environment

Integrating net-centric concepts into the information transport environment will require careful planning and collaboration across the Department. Changes in the environment will need to be reflected in policy, procedure and guidance to ensure that transport planning (capacity, quality of equipment/technology, redundancy) is fully supported. Transport's near-term focus is on:

- **Modularization** – Design solutions will be modularized, IP-based, and should consider historical usage patterns, location and mission focus. Proven configurations will emerge that can be mixed and matched based on mission need. The use of standardized bills of materials to support similar deployments will streamline the acquisition process resulting in faster deployment and/or augmentation of user locations. It will also reduce training requirements and promote confidence in the overall transport architecture.
- **Limiting Uniqueness** – Newer and broader-based technologies will provide opportunities, through replacement or retirement, to limit or eliminate non-standard equipment types/sets and their associated support requirements. This will facilitate the emergence of an interoperable network resulting in a reduction

in spare parts inventory, reduced maintenance (hardware and software) and repair costs and an optimization of opportunities for equipment reuse.

- **Rapid Deployment** – A modular, well known set of infrastructure equipment and configurations will enable rapid deployment of GIG capabilities in response to new mission requirements and/or arising tactical needs. This includes a comprehensive understanding of required resources to accomplish the complete deployment, enhancement, augmentation or re-deployment of a site.
- **Technology Evolution** - New technologies will require comprehensive testing to determine how they interact with existing systems and approved implementation methods. Newer technologies will support Internet Protocol version 6 (IPv6), network management Simple Network Management Protocol version 3 (SNMPv3) and capacity planning (modeling and simulation) which will guide decision makers in anticipating opportunities for establishing tiered network security, newer services and/or federating existing services.

Full testing of interoperability, equipment configuration (internal and interconnection), new technologies, and pilot programs will help ensure that the best equipment, services and modular deployments are kept current, constantly improved and are field ready. Embedding these elements within the DoD's acquisition processes will be one of the most critical factors in the Department's ability to realize an information transport environment that supports the goals of net-centric information availability.

Principles and Business Rules

The following principle and business rules are established to reduce complexity and cost, increase reliability, accommodate change, and implement GIG technical direction.

Communications Readiness Principle

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

Communications Readiness Business Rules

- Implement a modular, layered design based on Internet protocol for the transport infrastructure.
- 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.
- 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.
- 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 COIs.
- 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.
- Spectrum Management (SM) shall incorporate flexible, dynamic, non-interfering spectrum use.

NetOps Agility (NOA)

The vision of NetOps is to transform existing and new capabilities into a force multiplier that enable DoD to fully employ the power of the GIG. The corresponding mission is to enable the DoD to employ a unified, agile, and adaptive GIG that is:

- **Mission Oriented** – All information-dependent processes necessary for a mission can be effectively supported
- **User Focused** – Each user can access and obtain needed information from anywhere in the GIG in a timely manner; even when their needs are unanticipated
- **Globally Agile** – Rapidly changing mission priorities can be met by dynamically maneuvering GIG resources

Like much of the GIG, NetOps today is delivered through organizational and functional stovepipes with varying degrees of interoperability and information access. Each of these stovepipes has its own, largely independent management capability, which seldom shares information regarding the status of its management domain. The Joint NetOps Concept of Operations has enabled the DoD to begin significantly improving how the GIG is operated and defended. For NetOps to effectively play its role in enabling net-centric operations, however, major challenges will have to be addressed:

- GIG Situational Awareness information must be available to Commanders
- GIG Command and Control capabilities must support rapid decision making
- NetOps operational policies must be clear and well integrated
- NetOps must address the use of the electromagnetic spectrum
- Standardized metrics must measure the health and mission readiness of the GIG
- Capability development must be centrally governed
- Greater coordination or synchronization is required among the many independent NetOps acquisition and fielding activities currently under way

Addressing these challenges will significantly improve the ability of the operators and defenders of the GIG to fully support ongoing warfighting and peacekeeping missions in an increasingly joint and multi-partner environment.

Enabling NetOps Agility

In order to deploy robust NetOps capabilities in operational environments spanning organizational and geographic boundaries, the Department must leverage new thinking, new processes, new policies and new levels of cooperation across Components. To meet this challenge, NOA has established the following near-term goals:

- **Enable timely and trusted information sharing of NetOps information across the enterprise** – The fundamental premise is NetOps provides seamless, transparent flow of information (end-to-end) across the enterprise in response to user needs while ensuring GIG resources are provisioned and allocated in accordance with changing mission requirements. Achieving this goal is two fold:
 - Begin making NetOps data visible, accessible and understandable to all authorized users,
 - NOA must manage and facilitate the visibility, accessibility, understandability, and sharing of all information within and across all DoD missions.
- **Unify GIG Command and Control** – The DoD is increasingly dependent on the GIG as the primary means of enabling and delivering a wide variety of command and control (C2) to decision makers at all levels. Therefore it is critical the DoD transform the NetOps C2 construct by focusing on: increasing speed of command; implementing a decentralized policy-based construct for integrated management of all GIG domains and establishing consistent and coordinated Techniques, Tactics and Procedures (TTPs) for net-centric NetOps. Doing so will result in a NetOps C2 construct that operates and defend the GIG as a unified, agile and adaptive enterprise capable of maneuvering critical data, employing GIG capabilities when and where they are needed most, and rapidly changing the GIG configuration to significantly enhance the value of the GIG.
- **Evolve and mature NOA capabilities in stride with the capability delivery increments of the Net-Centric capability portfolio** – Time-phased NOA capability increments must be defined, developed and deployed in concert with the Net-Centric portfolio. In addition, NOA policy, governance structure, implementation plans and metrics must be created to achieve an effective transformation.

Principles and Business Rules

The following principles and rules have been established to provide a common foundation for tying together NetOps activities across the Department. While these guidelines are few in number, adherence to them across all applicable DoD IT investments will assist overall efforts significantly towards achieving the vision of NetOps Agility.

NetOps Agility Principle: Command and Control

- DoD shall operate and defend the GIG as a unified, agile, end-to-end information resource.

NetOps Agility Business Rules: Command and Control

- The DoD must continue to transform the NetOps 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.
- The DoD must ensure NetOps functions of Enterprise Management, Content Management, and Network Defense are fully integrated within and across all management domains.
- The DoD must conduct GIG NetOps functions at all operational levels (strategic, operational, and tactical).
- GIG programs must address relevant NetOps capabilities in Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF).
- 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.

NetOps Agility Principle: Situational Awareness

- 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: Situational Awareness

- 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.
- 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.

DoD IEA Products, Evolution, Future Challenges

DoD IEA 1.1 Products

This iteration of the DoD IEA focuses on establishing a baseline framework of principles and rules that guide the DoD Information Enterprise. Its core product is this architecture description document which:

- Explains the role of the DoD IE
- Places DoD IEA in the context of the Department's Federated Enterprise Architecture
- Establishes DoD Information Enterprise priorities for near-term decision making
- Defines core principles and business rules that should guide all investments
- Describes how to apply the DoD IEA content
- Describes compliance with the DoD IEA

This description documentation is complemented by a hierarchical activity model (an activity node tree), which decomposes each of the priorities into a set of core activities performed and/or governed by the DoD CIO. It may be accessed on the internet at URL: <http://www.defenselink.mil/cio-nii/sites/diea/>

It is here that the principles and rules laid out in the architecture description are tied to underlying DoD policies and guidance. The hierarchical activity model is linked both upward to DoD IE principles and rules, and downward to the constraints, mechanisms, and best practices that govern implementation activities. The activity model thus provides a means for users to use the activities to navigate the many policies and standards applicable to the GIG. The activity model also serves as a classification scheme for investment management and thus serves as an important linkage point between the DoD IEA and other DoD architectures for federation purposes.

DoD IEA Evolution

While DoD IEA 1.1 represents a strong beginning, it is by no means complete. Given the evolutionary nature of IT development, the DoD IEA is, and always will be, a work in progress. In the background section, it was stated that enterprise architectures and related guidance answer three questions:

- What must we do?
- How must we operate?
- When will we transition?

The DoD IEA 1.1 addresses the first two of these questions, building 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. The Department anticipates incorporating a transition plan in parallel with

future releases of the DoD IEA to provide guidance that addresses when and how DoD will transition.

It is not expected that future releases will include a significant increase in the number of formal architecture products. Existing products will be refined, and additional operational views (particularly process models) may be included to demonstrate enterprise-wide solutions to specific DoD IT problems. Certain types of views, however, will likely never be included in the DoD IEA. For example, logical data models and traditional systems views are inconsistent with the DoD Data and Services strategies as well as the overall concept of net-centric information sharing. These architecture products, however, may well be appropriate for capability or Component architectures given the challenges of managing the transition from the legacy environment.

The Challenge Forward

The principles and rules outlined in DoD IEA 1.1 are few, but powerful. As they are embedded in decision-making processes across DoD, and applied to DoD investments, they will accelerate the Department's evolution to net-centric information sharing. The key focus for the architecture going forward is institutionalizing its rules and principles across the Department. Steps towards institutionalization are in progress. The Department is:

- Focusing on supporting decision makers across the Department in using the DoD IEA as a tool to appropriately guide and constrain the IT investments for which they are responsible.
- Accelerating the evolution of the COI approach to solving data, information and services issues facing the Department.
- Addressing and resolving issues related to the funding and sustainment of the enterprise services model of operations.

A near-term priority for the DoD CIO is merging related enterprise architecture guidance into the DoD IEA. This merger will provide a common, easily understood framework for critical architecture guidance.

Achieving the goals of net-centric operations will require sustained commitment across all layers of the DoD. DoD IEA 1.1 is an important step in DoD's net-centric transformation – one that ensures efforts are aligned to achieving a common vision.

(This page intentionally left blank)

Appendix A. DoD IEA Principles and Business Rules

DoD IEA Global Principles (GP)

- GP 01 - DoD 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 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. 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.

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, 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 - 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 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.

Secured Availability Principle (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.

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 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.

Secured Availability Principle (SAP)

- 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 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.

Secured Availability Business Rule (SAR)

- SAR 05 - GIG assets must establish and implement a Mission Assurance capability that addresses hardware, software and supplier assurance through engineering and vulnerability assessments.

Secured Availability Principle (SAP)

- 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 Defense Information Enterprise.

Secured Availability Business Rules (SAR)

- 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.

Secured Availability Principle (SAP)

- SAP 04 - Agility and precision are the hallmark of twenty-first 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 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 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 manageable rapidly 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 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)

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

Communications Readiness Principle (CRP)

- CRP 01 - The GIG communications infrastructure shall support full 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 Principle: Command and Control (NOAP)

- NOAP 01 - DoD shall operate and defend the GIG as a unified, agile, end-to-end information resource.

NetOps Agility Business Rules: Command and Control (NOAR)

- NOAR 01 - The DoD must continue to transform the NetOps 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.

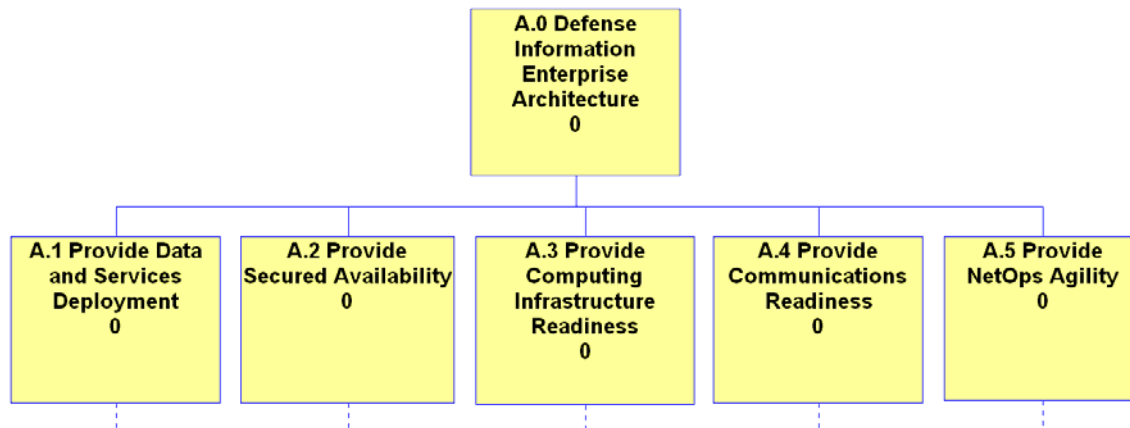
NetOps Agility Principle: Situational Awareness (NOAP)

- 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: Situational Awareness (NOAR)

- 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.

Appendix B: DoD IEA Hierarchical Activity Model



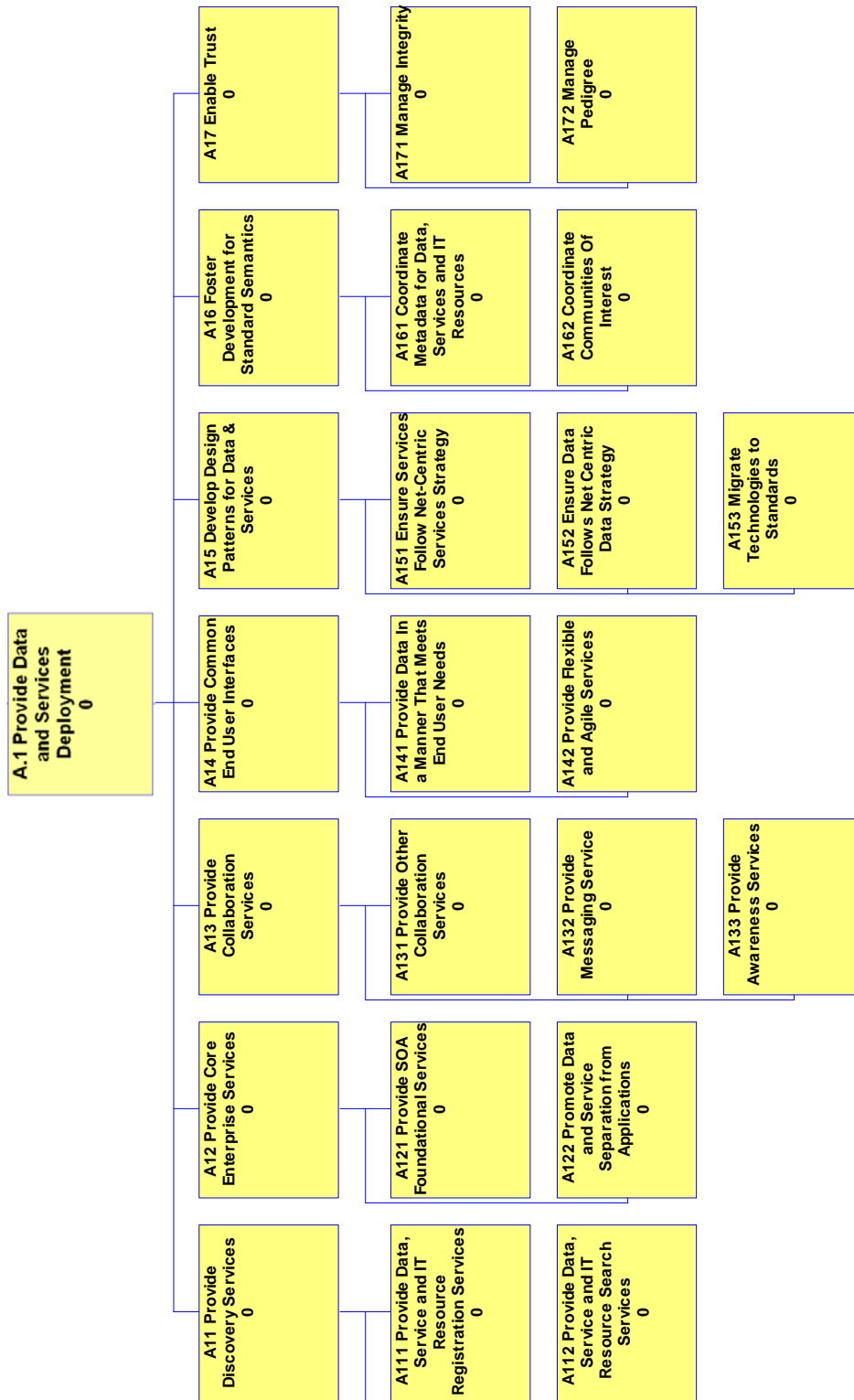
As mentioned in the Executive Summary and Introduction sections, this architecture contains a hierarchical activity model (activity node tree), which decomposes each of the five priorities into a set of core activities performed and/or governed by the DoD CIO. The node tree's five branches represent the core activities associated with each of the five priorities. This appendix is intended to provide a quick reference when reviewing the architecture.

The hierarchical activity model is designed to facilitate linking leadership intent with implementation-level guidance. Each activity node within the hierarchical activity model is linked both upward to DoD IEA principles and rules, and downward to the DoD plans, policies, strategies, mechanisms, and best practices that govern net-centric transition. The activity model thus provides a means for users at multiple levels to rapidly abstract requirements from the many policies and standards applicable to the GIG.

To access this information, visit the DoD IEA website at: <http://www.defenselink.mil/cio-nii/sites/diea/>

- Under the banner *DoD IEA 1.1 Products*, click the link entitled *Hierarchical Activity Model*.
- Click on an activity node that will link you to a view of that activity's parent and children activities, as well as its associated principles, rules, constraints, mechanisms, and best practices.
- Downloadable versions of the model, activity descriptions, principles and rules, a glossary of terms and acronyms, and other supplemental information are available.

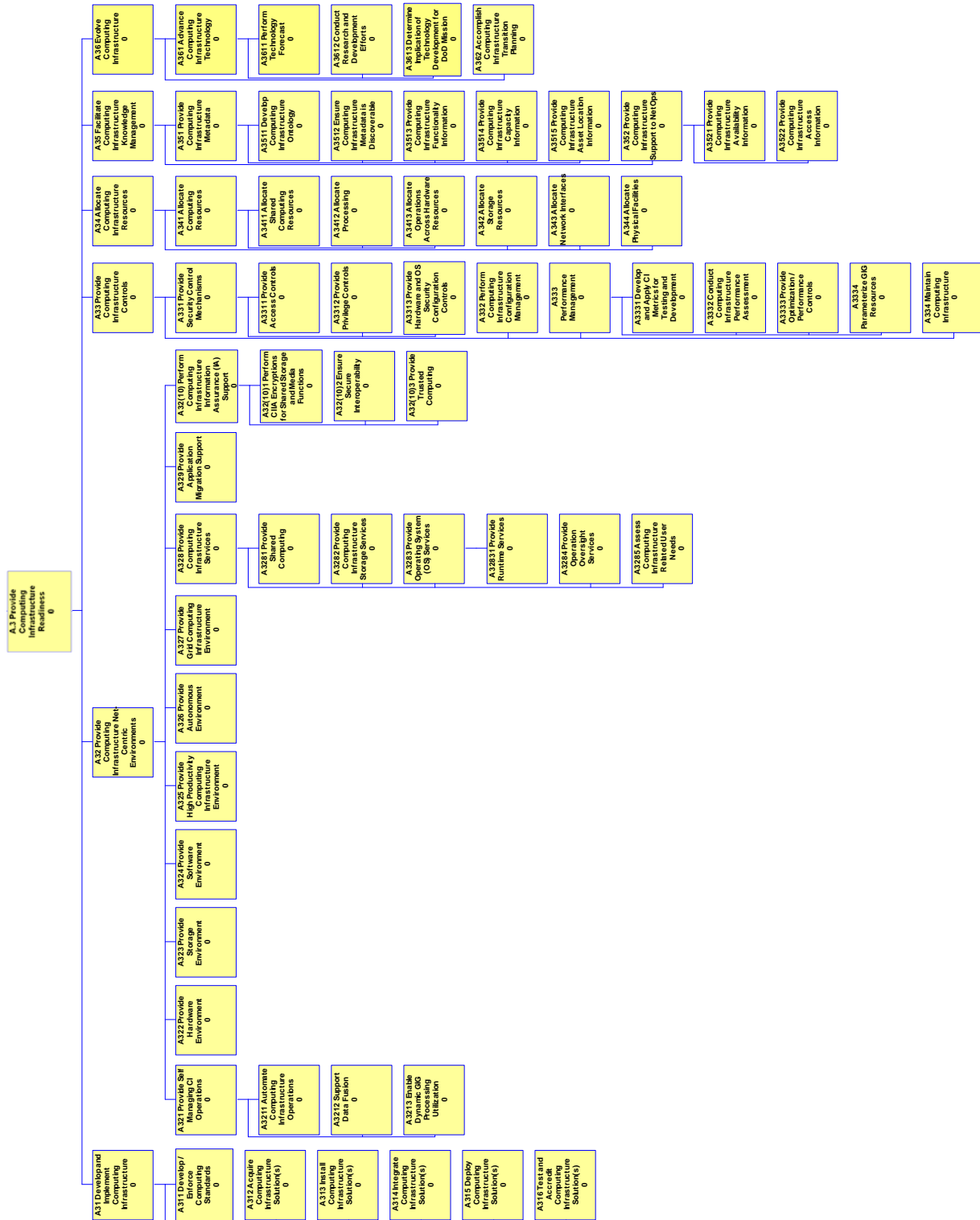
Appendix B: DSD (Cont)



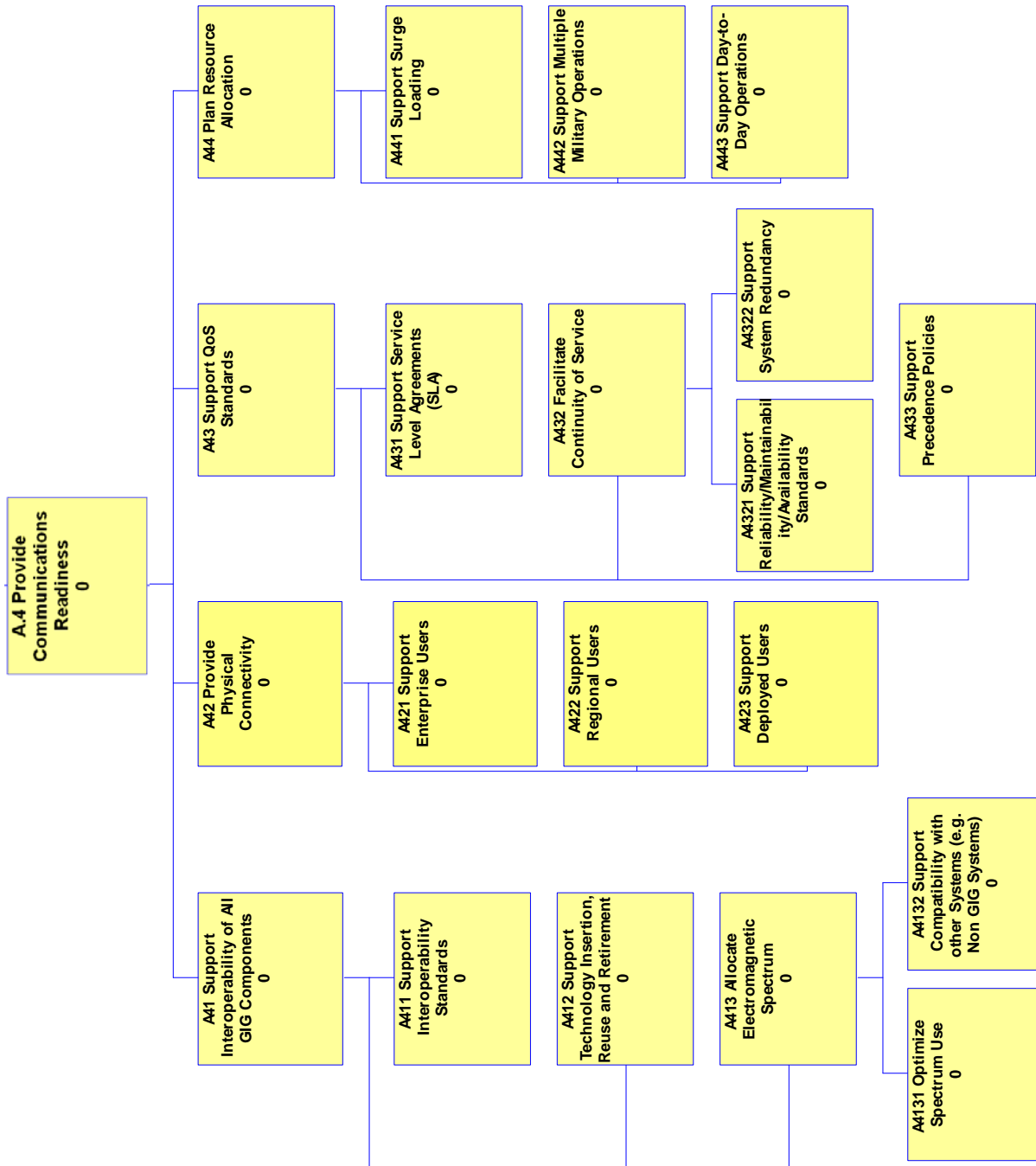
Appendix B: SA (Cont)



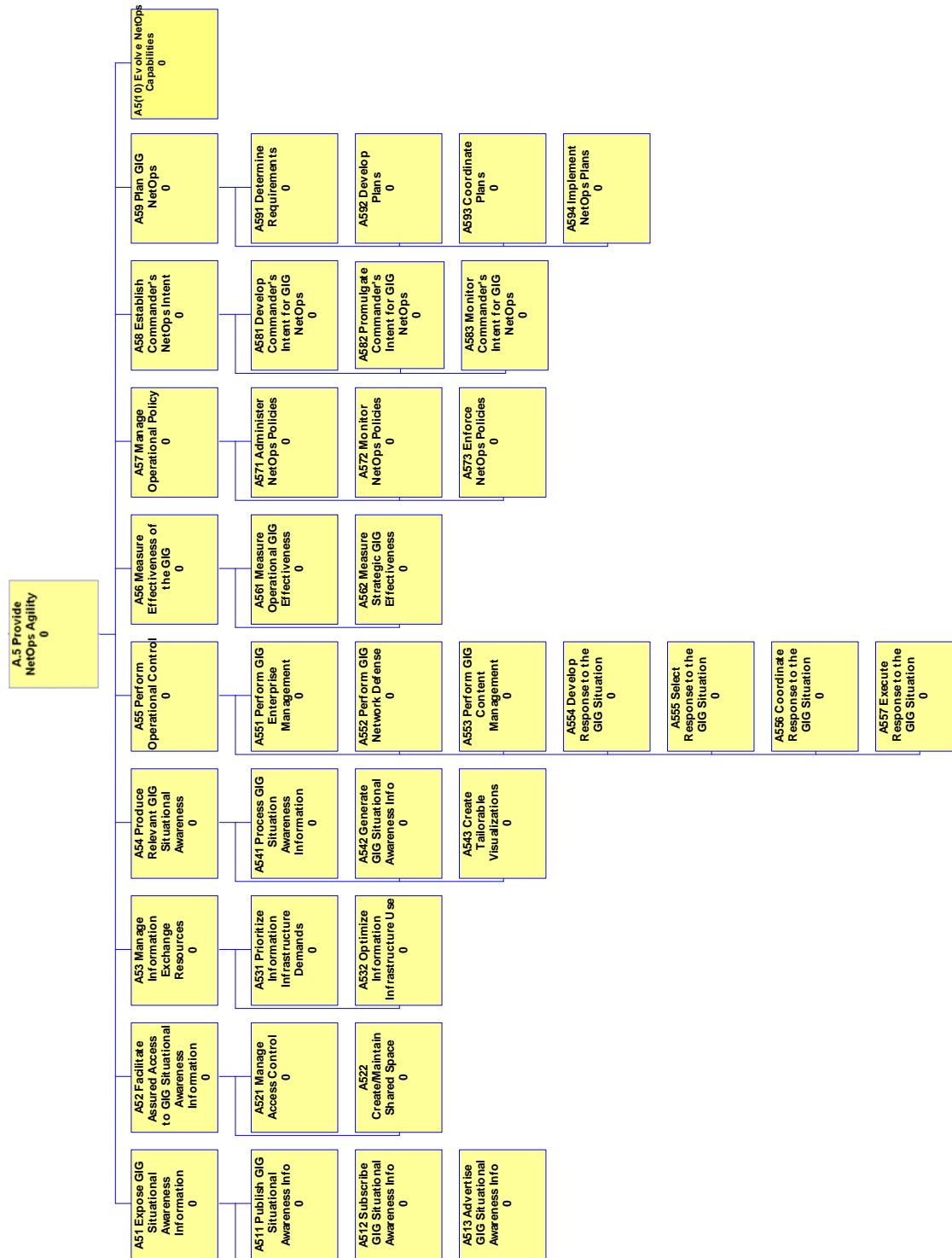
Appendix B: CIR (Cont)



Appendix B: CR (Cont)



Appendix B: NOA (Cont)



Appendix C: Acronyms

C2	Command and Control
CI	Computing Infrastructure
CIO	Chief Information Officer
CIR	Computing Infrastructure Readiness
COCOM	Combatant Command
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	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities
DSD	Data and Services Deployment
FEA	Federal Enterprise Architecture
GCN	GIG Computing Node
GIG	Global Information Grid
IA	Information Assurance
IC	Intelligence Community
IM	Information Management
IP	Internet Protocol
IPv6	Internet Protocol version 6
IRB	Investment Review Board
IT	Information Technology

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

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

1. Introduction

This appendix describes an approach for applying the DoD IEA in support of three distinct types of customer: IT Architects; Managers of IT Programs, to include DoD and Component Program Executive Officers (PEOs), Program Managers (PMs), and their corresponding functional requirements managers; and IT Decision-Makers, to include Capability Portfolio Managers (CPMs), Investment Review Boards (IRBs), CIOs, and others. This approach allows the DoD IEA to support the linking of IT investments and acquisitions to explicit operational gaps or mission needs. **Figure D-1**, Applying DoD IEA, provides an overview of the application approach.

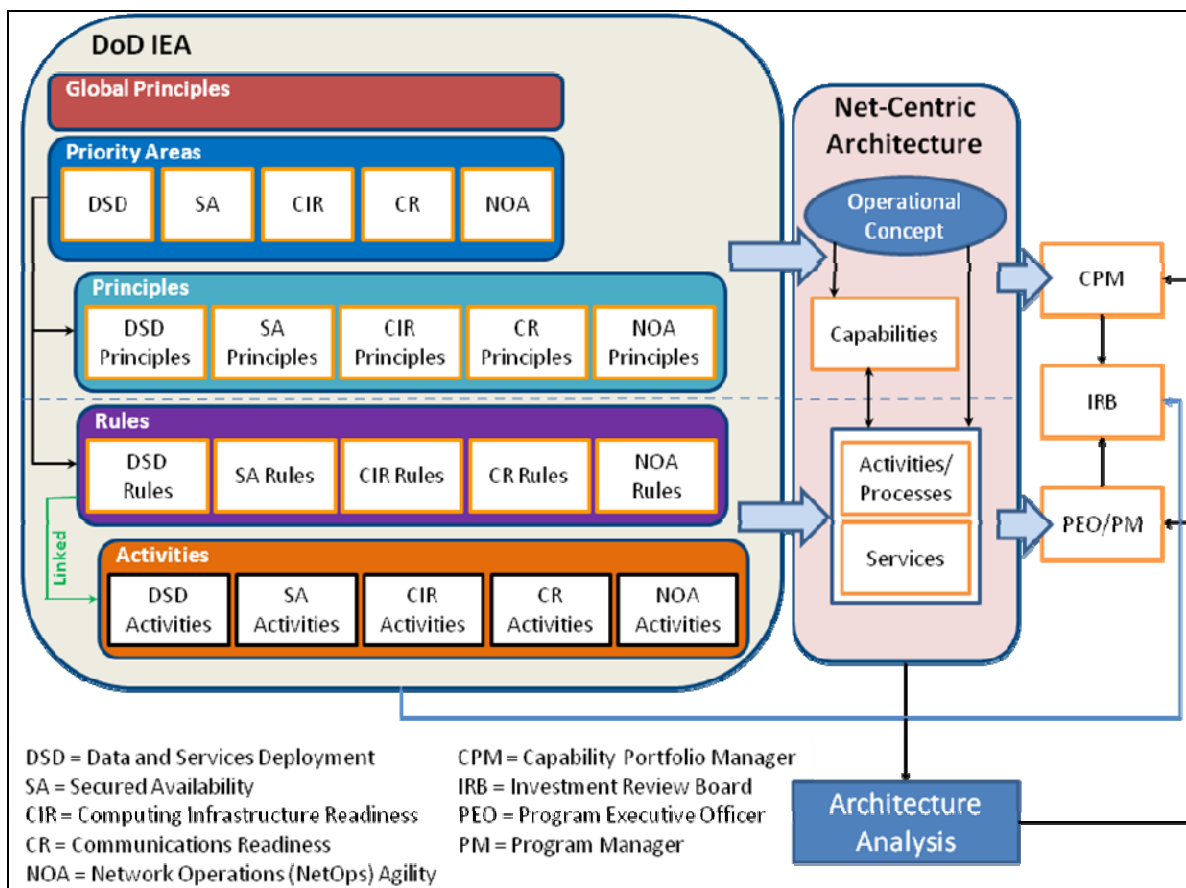


Figure D-1 - Applying the DoD IEA

The approach emphasizes applying DoD IEA to the production of net-centric architecture descriptions¹ by aligning with key DoD IEA elements. The information from these net-centric architecture descriptions, along with that from proper architecture analysis, is then applied in support of IT investment decision-making and program development and execution.

The following sections describe this approach in more detail, beginning with an extensive discussion of alignment with key net-centric elements of the DoD IEA by architecture descriptions at all DoD tiers (Enterprise, Component, and/or Program)². This discussion is then followed by separate descriptions of how PEOs/PMs can use net-centric architectures to enable development, acquisition, and fielding of effective net-centric capabilities for the warfighter, and how decision-makers, to include CPMs and IRBs, can use such architectures to evaluate investments and programs.

2. Applying DoD IEA in Architecture Development and Maintenance

This section presents a process for applying DoD IEA in the development and maintenance of net-centric DoD architectures. The process describes how the DoD IEA should be used to shape architectures so they correctly reflect net-centric characteristics of the “to be” DoD Information Enterprise (IE). It is not a “step-by-step” guide for building net-centric models or views. Instead, it identifies what an architect³ needs to know about net-centric operations and information sharing and then how to apply that knowledge in developing and maintaining net-centric architecture descriptions.

The DoD IEA is the means for aligning all DoD architectures with the Department’s net-centric concepts, strategies, policies, and guidance so those architectures can enable net-centric operations identified, assessed, and prioritized by the DoD JCIDS process; resourced by DoD’s PPBE process; and with the support of materiel acquisitions obtained via the Defense Acquisition System (DAS) process. Although examples in the following subsections focus on application of the DoD IEA to DoDAF-defined architecture descriptions, the approach presented here applies to any architecture description, regardless of its structure and the method used to develop it.

The process described here requires the architect to understand and use a complementary and foundational knowledge base of net-centric concepts, to include those described by the DoD C4ISR Cooperative Research Project (CCRP); addressed in the Net-Centric Environment (NCE) Joint Functional Concept (JFC) and the Net-Centric Operational Environment (NCOE) Joint Integrating Concept (JIC) and Joint Capabilities Document (JCD); and encompassed by

¹ DoDAF v1.5 (Volume I, p. 1-6) defines an architecture description as “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.”

² These tiers are the ones described in Defense Information Enterprise Architecture (DIEA) v1.0, 11 Apr 2008, p. 3.

³ The term architect is used here to mean any group, individual, and/or organization within DoD responsible for developing and maintaining, governing, and/or supporting the use of architectures.

technical federation, SOA, and technology innovation best practices. The process further aligns DoD architecture descriptions with the Joint Capability Area (JCA) taxonomy for use in locating attributes and requirements for effective net-centric information sharing. Finally, the process stresses the use of net-centric architecture analyses to develop more detailed guidelines, derived from Principles and Rules in the DoD IEA, to direct IT investments and programs to achieve the Department's net-centric objectives.

2.1 Where to Apply the DoD IEA

The DoD IEA should be applied to all architecture descriptions wherever they define interaction with the DoD IE. Alignment of architecture descriptions with the DoD IEA supports achievement of the Department's Net-Centric Vision and associated goals and objectives. It is essential to understand that the DoD IEA applies to all Capability Portfolios, not just the Net-Centric one. For this reason, all capability architectures should be aligned with the DoD IEA (where appropriate) in accordance with the approach presented here. **Figure D-2**, Where to Apply the DoD IEA, depicts where the DoD IEA should be applied. This diagram shows the primary elements of the DoD IEA (Priority Areas, Principles, Rules, Activities, Constraints, and Mechanisms) that should be applied to an architecture, based on tier and type.

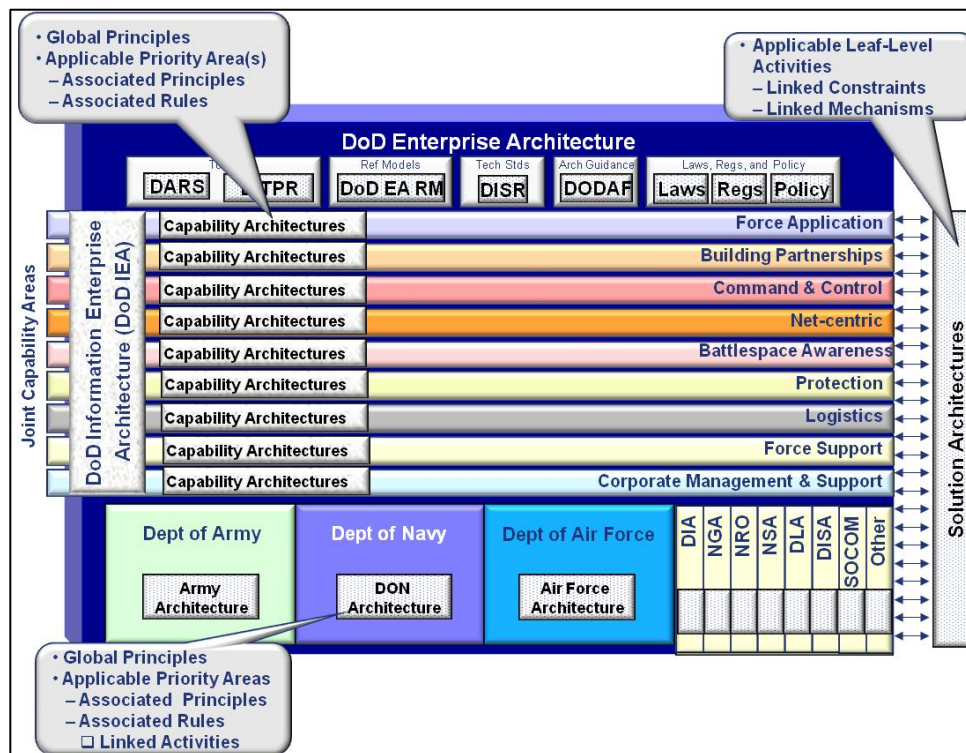


Figure D-2 - Where to Apply the DoD IEA

Descriptions of Priority Areas⁴ in the DoD IEA provide Department architects with a common vision of the net-centric information environment in key areas where capabilities are most needed. The DoD IEA Principles, Rules, and Activities provide common constraints for use in all DoD architecture descriptions to direct how operations are conducted, services function, and data is processed and used in the net-centric DoD IE. The DoD IEA elements shown in the diagram as applicable to a specific architecture tier and type are considered the minimum necessary to describe interactions with the net-centric information environment at that level. This does not preclude use of additional DoD IEA elements to ensure a more complete, accurate, and/or detailed picture of the DoD IE to meet a given architecture's purpose, viewpoint, and scope.

The Department's concepts of Tiered Accountability and Federation require architectures at each tier to align and comply with applicable aspects of architectures at higher tiers. This requirement to align architectures across tiers means an architect must incorporate applicable net-centric elements and guidance from higher level architectures. Because these higher level architectures must also align with the DoD IEA (where applicable) this requirement extends the DoD IEA, providing architects at lower tiers with additional detail on the net-centric aspects of the DoD IE, as described in higher level architectures. Such an alignment across tiers allows the content of the DoD IEA to be supplemented and interpreted to meet the needs of architects at lower tiers, while supporting a tracing of net-centric aspects in any given architecture back through higher level architectures to the DoD IEA.

As shown in **Figure D-3, Approach for Applying DoD IEA**, the basic approach for applying the DoD IEA to a DoD architecture is essentially the same, regardless of the tier or type architecture involved. But because the applicable content of the DoD IEA, and exactly how that content is applied, does vary with the architecture tier and type, the next subsections describe any differences in alignment required for a given architecture.

⁴ Priority Areas are defined on p. 6 of DIEA v1.0. The five Priority Areas are: Data and Services Deployment (DSD), Secured Availability (SA), Computing Infrastructure Readiness (CIR), Communications Readiness (CR), and NetOps Agility (NOA).

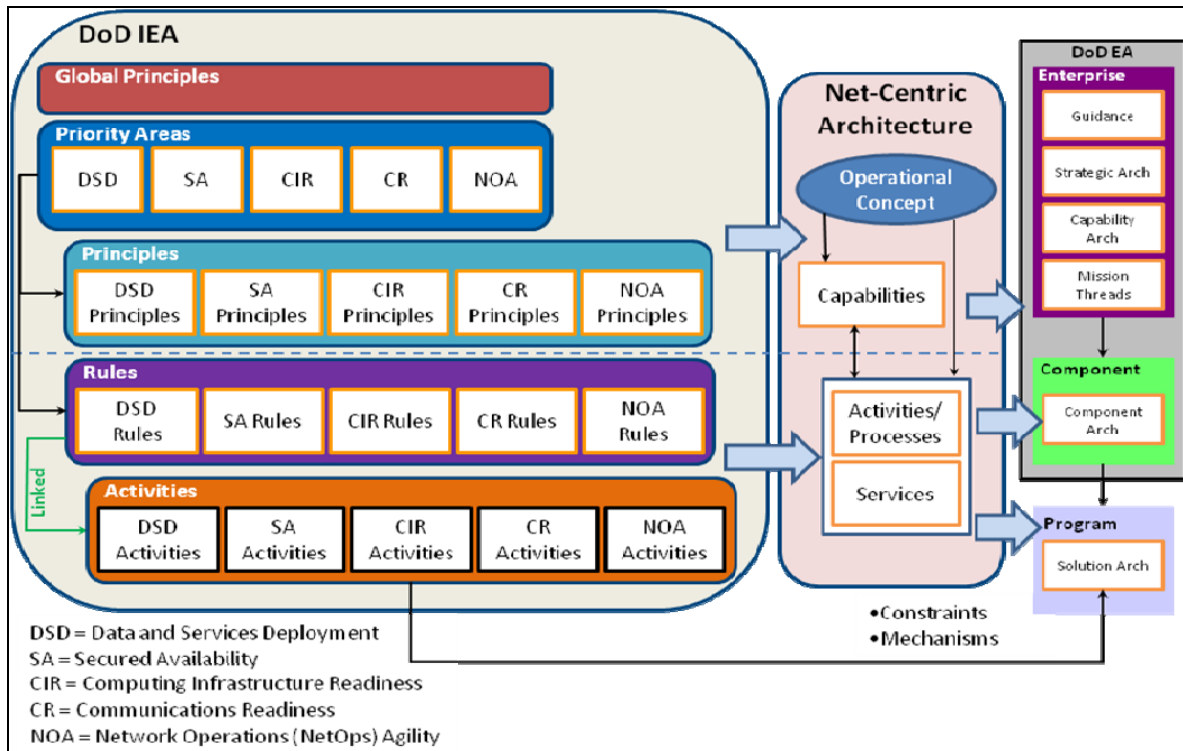


Figure D-3 - Approach for Applying the DoD IEA

2.2 Process for Applying DoD IEA to DoD Architectures

Figure D-4, Process for Applying DoD IEA to DoD Architecture Federation, is a conceptual process flow for applying the DoD IEA to the development, maintenance, and use of net-centric architecture descriptions within the DoD Architecture Federation. The diagram presents a high-level template or pattern for applying the appropriate DoD IEA Priority Areas, Principles and Rules, Activities, and Constraints and Mechanisms; components of complementary net-centric enabling concepts; the JCA taxonomy; and related net-centric terminology (from approved vocabularies and taxonomies) in building net-centric architecture descriptions. The diagram shows primary inputs above and sub-processes below each of the main process step boxes.

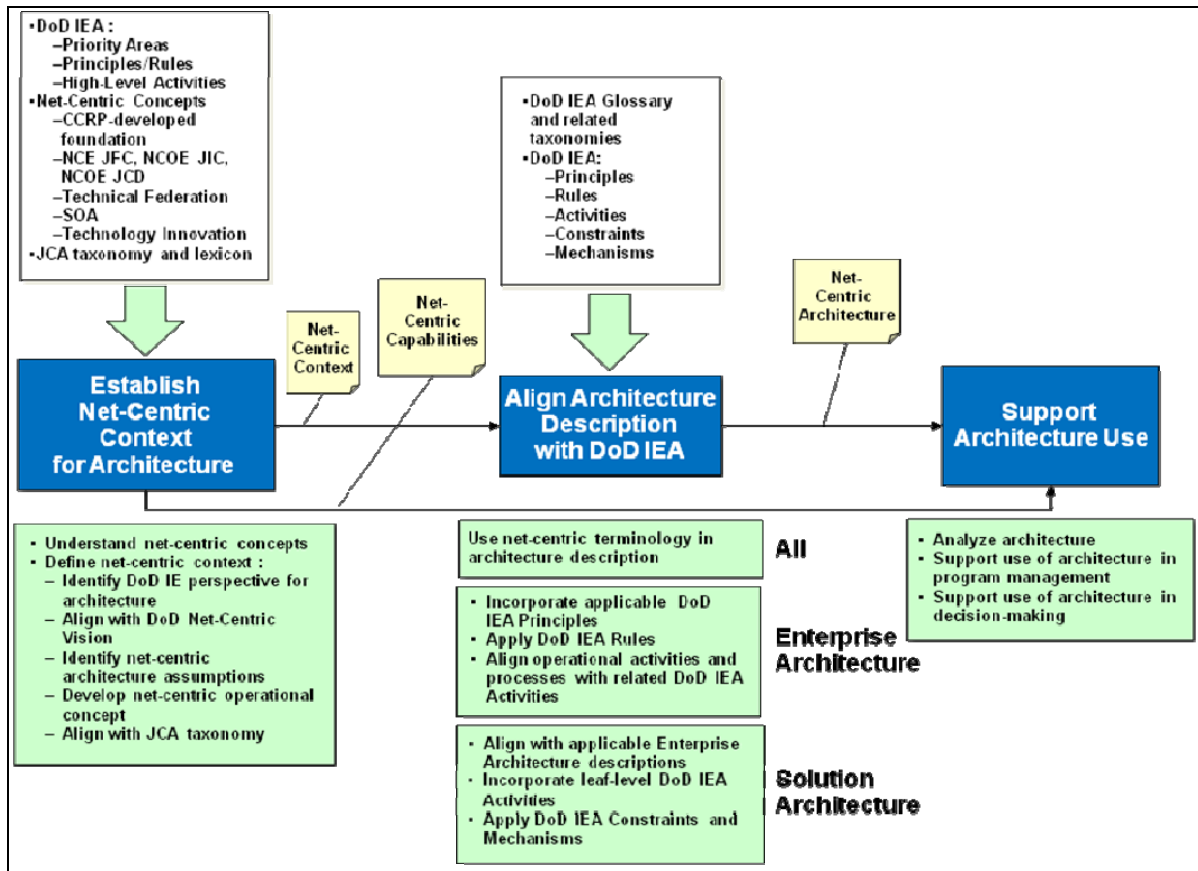


Figure D-4 - Process for Applying DoD IEA to DoD Architectures

Each of these steps and their associated sub-processes are described in greater detail in the next section. The main process steps can be summarized as:

- **Establish Net-Centric Context for Architecture** – The architect obtains a basic understanding of net-centric operations and information sharing and the DoD IE by studying foundational net-centric concepts developed by the CCRP; future joint concepts as developed in accordance with CJCSI 3010.02; characteristics of DoD-accepted net-enabling concepts of technical federation, SOA, and technology innovation; the net-centric aspects of the DoD IE described by the DoD IEA; and capabilities from the JCA taxonomy. Based on this understanding, the architect identifies the portions of the Department’s Net-Centric Vision applicable to the architecture, applies appropriate DoD IEA Priority Areas, Principles and Rules, and high-level Activities to the development of a net-centric context for the architecture, and aligns this context with the JCA taxonomy in support of locating and using appropriate net-centric attributes and requirements in the architecture description.
- **Align Architecture Description with DoD IEA** – Using the net-centric context established in the previous step, the architect develops an architecture description aligned with the DoD IEA. For all architectures, the architect should use net-centric vocabulary from the Net-Centric JCA taxonomy and the DoD net-centric strategy

documents in describing architecture elements and relationships. For Enterprise architecture descriptions, the architect identifies pertinent DoD IEA Principles and applies them to the architecture in describing interactions with the net-centric DoD IE; selects DoD IEA Rules appropriate to the applicable Principles; and uses these Rules to align activities and processes defined by the architecture to applicable DoD IEA Activities. For solution architecture descriptions, the architect aligns with the net-centric elements of applicable enterprise architectures, then selects and applies appropriate leaf-level DoD IEA Activities and related Constraints and Mechanisms where needed to address gaps and meet requirements of the solution space.

- **Support Architecture Use** – The architect analyzes capability, component, and solution architectures in conjunction with program managers and decision-makers to develop a set of net-centric guidelines, conformant with DoD IEA Principles and Rules as applied in governing capability and component architecture descriptions, to provide more detailed direction for program management and criteria for decision-making assessments. The architect then supports these stakeholders in using this net-centric guidance and information provided by the appropriate net-centric architecture descriptions in the development, acquisition, and deployment of required net-centric capabilities.

2.3 Applying DoD IEA to DoD Architectures

The process steps for applying DoD IEA in DoD architecture development and maintenance, as shown in the conceptual process flow, are described in more detail here. Included in each of the following subsections is a description of the individual sub-processes occurring within the given process step. Descriptions of the processes for using the resulting net-centric architectures to enable program management and decision-making are contained in Sections 3 and 4, respectively.

2.3.1 Establish Net-Centric Context for Architecture

This step provides the architect with a basic understanding of net-centric operations and information sharing in general, and the net-centric aspects of the DoD IE in particular, as a basis for developing architecture descriptions aligned with the Department's Net-Centric Vision. The architect uses this understanding to establish a net-centric context for the architecture. This net-centric context, instantiated in architecture assumptions, the operational concept driving the architecture, and net-centric capabilities from the JCA taxonomy, establishes the proper net-centric scope for the architecture.

2.3.1.1 Understand Net-Centric Concepts

The architect should first obtain a good understanding of net-centric operations as a basis for determining how to apply the DoD IEA to architectures to enable such operations. This process should start with a thorough review and understanding of the theoretical foundation for net-centric operations. The DoD CCRP has published such a theoretical foundation of net-centricity in its Net-Centric Warfare (NCW) series of books. To date, these books are: *Network Centric Warfare*, Alberts, Garstka, and Stein (1999); *Understanding Information Age Warfare*, Alberts, Garstka, Hayes, Signori (2002); *Information Age Transformation*,

Alberts (2002); *Power to the Edge*, Alberts and Hayes (2003); and *Complexity Theory and Network Centric Warfare*, Moffat (2003).⁵ By reviewing the theories and abstract concepts described in these books, the architect will gain a basic understanding of the core attributes of net-centric operations as a starting point for understanding and applying net-centric information sharing in support of these operations.

This theoretical understanding should then be used to gain an understanding of the more detailed concepts for net-centric operations and information sharing defined across DoD. Such concepts have been defined as part of the Joint Operations Concept Development Process (JOpsC-DP), described in CJCSI 3010.02B (27 January 2006), which develops joint future concepts linking “strategic guidance to the development and employment of future joint force capabilities.” This process includes joint experimentation, “an iterative process for assessing the effectiveness of varying proposed joint warfighting concepts, capabilities, or conditions,” to recommend development of new concepts, revision of existing concepts, or changes in DOTMLPF and policy to “achieve significant advances in future joint operational capabilities.”

The JOpsC family of documents, consisting of the Capstone Concept for Joint Operations (CCJO), Joint Operating Concepts (JOCs), Joint Functional Concepts (JFCs), and Joint Integrating Concepts (JICs), looks beyond the Future Years’ Defense Plan (FYDP) out to twenty years. These documents, while being informed by existing “to be” DoD architectures, also provide the descriptions of future functions, environments, and operations that form the context for architectures across the Department. Department architects, therefore, should apply appropriate future concepts from the JOpsC family in development, analysis, and use of their architectures.

With respect to net-centric operations and information sharing, the JOpsC-DP has developed specific concepts which architects must understand and apply in developing net-centric context for Department architectures:

- **Net Centric Environment Joint Functional Concept (NCE JFC)**, August 2005, describes how “joint forces might function in a fully networked environment 10 to 20 years in the future.”
- **Net-Centric Operational Environment Joint Integrating Concept (NCOE JIC)**, October 2005, describes a Net-Centric Operational Environment providing “the technical connectivity and interoperability necessary to rapidly and dynamically share knowledge among decision-makers and others—while protecting information from those who should not have it.”

This is not to say other JOpsC documents are not applicable to developing net-centric context for an architecture. To the contrary, implementation of the Department’s Net-Centric Vision requires the application of net-centric attributes and requirements to the definition of all future

⁵ Hard copies of these books can be obtained free of charge using order forms on, or soft copies can be downloaded in Adobe Acrobat format from, the CCRP web site (<http://www.dodccrp.org/>).

operational concepts across the Department. Consequently, every JOpsC document should apply net-centric concepts specific to the functions, environment, and/or integrated operations it describes. For this reason, an architect should review all pertinent JOpsC documents to understand just how net-centric concepts apply to the architecture being developed, analyzed, and/or used. In conjunction with the NCE/NCOE joint concepts previously described, understanding of the net-centric aspects present in all pertinent joint concepts can then be appropriately applied to the architecture and its use.

Additional understanding of the net-centric capabilities, their attributes and requirements, necessary for net-centric operations can be obtained from the Joint Capabilities Document for the Net-Centric Operational Environment (NCOE JCD), v1.0, 15 December 2006. This document, derived from the NCE JFC and NCOE JIC, “defines the baseline functional capabilities and attributes for future Joint Net-Centric Operations (JNO) at all levels of command and across the range of military operations (ROMO).” Used in conjunction with the Net-Centric JCA taxonomy and lexicon, this document provides the architect with an understanding of the capabilities necessary to support and enable the net-centric operational concepts defined by the JOpsC-DP.

Finally, the architect should become familiar with three key DoD-accepted concepts for enabling net-centric information sharing – technical federation, SOA, and technology innovation. These enabling concepts are defined and described in a number of policy, guidance, and strategy documents, and are evolving and maturing with the overall net-centric direction in the Department. The three enabling concepts can be summarized as follows:

- **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 such areas as identity management, digital trust, management of name spaces/directory structures, and security enclaves.
- **Service Oriented Architecture (SOA)** is the vision defined in DoD’s Net-Centric Services Strategy (NCSS). The SOA concept allows the Department to create an agile enterprise with services available across the Department for sharing information – information created by executing service-enabled mission and business processes. The SOA concept covers such areas as the creation of a Service Oriented Enterprise (SOE), service implementation and employment, development and fielding of a SOA Foundation (SOAF), to include core enterprise services; and service discovery and orchestration.
- **Technology Innovation** involves the specification of target information technologies, and associated relationships that will contribute 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.

With the background provided by all of these foundational documents and their concepts, the architect can read and absorb the DoD IEA to gain a thorough understanding of the net-centric characteristics of the DoD IE. The DoD IEA helps to clarify how the concepts embedded in the Department's acquisition strategies are expected to achieve the priorities identified by the formally-established JCIDS operational needs. Because the DoD IEA has integrated and consolidated the DoD Net-Centric Strategies and other foundational policy and guidance documents governing net-centric information sharing, it represents the authoritative source for the description of and requirements for the DoD Net-Centric Vision. However, during architecture planning, development, and use, it may be necessary for the architect to also consult the foundational policy and guidance documents themselves to obtain additional detail in specific areas of this vision. In addition to those already mentioned, these foundational documents include the DoD Information Sharing Strategy, the GIG Architectural Vision, and the full range of net-centric DoD directives and instructions.

As architecture development, maintenance, analysis, and use proceeds, the architect should use the additional net-centric knowledge contained in the CCRP writings, joint future concepts, NCOE JCD and Net-Centric JCA, and the enabling concepts of technical federation, SOA, and technology innovation to complement the DoD IEA's description of Priority Areas, Principles, and Rules for better understanding the net-centric aspects of the DoD IE. The architect should also apply this additional net-centric knowledge to supplement information in the DoD IEA in defining requirements for net-centric capabilities.

2.3.1.2 Identify DoD IE Perspective of Architecture

One of the keys to successful net-centric operations is proper interaction with the DoD IE. To align with the DoD Net-Centric Vision, DoD architectures must properly describe this interaction. Interaction with the DoD IE involves:

- Production/provision of data and services (i.e., the architecture describes how data and services are developed and provided to users)
- Management/operation of data and services (i.e., the architecture describes how data and services are managed or controlled)
- Consumption/use of data and services (i.e., the architecture describes how data and services are used)

The architect uses the identified purpose and scope of the architecture to determine where and how the architecture should interact with the DoD IE. These interactions result in the architecture describing different perspectives of the DoD IE – provider, manager, and consumer of information services. Each architecture description will need to address a combination of these perspectives, and the perspective of the architecture is likely to change

at different points in the architecture description. The architect uses these perspectives to determine how to apply DoD IEA Priority Areas, Principles, Rules, and Activities, in the architecture description. As appropriate, subsequent descriptions of process and sub-process steps point out distinctions in how DoD IEA elements are applied to address differences in DoD IE perspectives.

2.3.1.3 Define Net-Centric Context

The architect uses the previously gained understanding of net-centric concepts and the DoD IE to develop a net-centric context for use in developing an architecture description aligned with the DoD IEA and reflecting proper perspectives of the DoD IE. This context includes net-centric assumptions, a net-centric operational concept, and alignment with standard net-centric capability definitions. The net-centric context guides architecture development so the architecture description will properly present net-centric characteristics appropriate to the architecture's purpose, viewpoint, and scope.

2.3.1.3.1 Align with DOD Net-Centric Vision

To enable proper provision, management, and use of the DoD IE, architectures need to conform to the DoD Net-Centric Vision. As presented in the DoD IEA, this Vision is “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.
- An available and protected network infrastructure (the GIG) that enables responsive information-centric operations using dynamic and interoperable communications and computing capabilities.”

This alignment will be achieved by addressing how the architecture meets the challenges to the Vision described by the DoD IEA Priority Areas and through proper application of the associated Principles and Rules in the architecture description. The architect uses the perspectives the architecture takes of the DoD IE to determine how to address the Priority Areas in the architecture, and in later selecting and applying associated Principles and Rules to align the architecture description with the DoD IEA. To align with the Net-Centric Vision, the DoD IEA Priority Areas should be addressed as follows:

- **Data and Services Deployment (DSD)** and associated Principles and Rules should be used to define how data and services are provided and managed so they are separated from the applications and systems supplying them and to meet the needs of both identified and unanticipated users. The DSD describes key requirements for achieving SOA.
- **Secured Availability (SA)** and associated Principles and Rules should be used to define how data and services are provided and managed so they can be trusted across DoD; how consumers, based on their authorizations, will access discovered data and

services; and how permissions and authorizations are provided and managed so they are able to follow consumers wherever those consumers are on the network. Secured Availability describes how security is provided so security issues do not hinder authorized access to authentic information.

- **Computing Infrastructure Readiness (CIR)** and associated Principles and Rules should be used to define the provision and management of the computing infrastructure and related services so DoD can operate according to net-centric concepts. The CIR description also defines for consumers the infrastructure services available to them for processing and storage of data in a net-centric environment, and how the DoD IE will dynamically respond to computing needs and dynamically balance loads across the infrastructure.
- **Communications Readiness (CR)** and associated Principles and Rules should be used to define how an evolvable transport infrastructure is to be provided and managed to dynamically supply the required bandwidth and access for all capabilities operating in the DoD IE. The CR Priority Area further defines for consumers the end-to-end, seamless, net-centric communications capability expected to be available for their use across the DoD IE.
- **NetOps Agility (NOA)** and associated Principles and Rules should be used to define requirements for the management of the network and infrastructure capabilities enabling consumers to easily access, manipulate, manage, and share information from any location, at any time. The NOA Priority Area defines policies and priorities for operating and defending the GIG. It further describes common processes and standards for use in governing operations, management, monitoring, and response for the DoD IE.

2.3.1.3.2 Identify Net-Centric Architecture Assumptions

Net-centric assumptions for the architecture should be derived from the descriptions of the DoD IEA Priority Areas and should encompass applicable Principles and Rules. The assumptions should take into consideration related direction provided by foundational policy and any applicable requirements associated with the technical federation, SOA, and technology innovation concepts. In addition, the assumptions will need to take into account the perspectives the architecture takes of the DoD IE:

- Where the architecture describes the production/provision and/or management/operation of data and services, net-centric assumptions should be defined for how providers develop, acquire, deliver, or manage and operate their capabilities. Assumptions to address the provider and manager perspectives might also be developed from technical federation, SOA, and technology innovation concepts.
- Where the architecture describes consumption/use of data and services, net-centric assumptions should be defined for how information sharing elements are accessed and used. The SOA and technology innovation concepts are also good sources for

assumptions in this regard, since they describe requirements for the use of services and the technology on which consumers rely to enable net-centric operations.

2.3.1.3.3 Develop a Net-Centric Operational Concept

An operational concept should be at the heart of every DoD architecture, setting its scope and context and aligning it with DoD operational requirements, direction, and guidance. In order for an architecture to maintain its proper focus on the Department's Net-Centric Vision, therefore, its operational concept must contain guidelines and direction for the conduct of net-centric operations. It must also describe how the DoD IE is used to enable such operations.

A key to developing the proper net-centric context for the architecture, then, is to incorporate the Net-Centric Vision into the operational concept. This requires adding appropriate elements from the DoD IEA to the operational concept description so it addresses how net-centric operations are accomplished in the DoD IE. The DoD IEA Priority Areas and associated Principles and Rules provide guidelines for net-centric information sharing in the conduct and support of net-centric operations. Incorporating these descriptions, where appropriate, into the operational concept will bind the architecture so it expresses net-centric intentions for directing IT design and investment decisions. By including descriptions of associated high-level DoD IEA Activities into the operational concept, the architect can also show how operations are conducted to effectively provide, manage, and consume data and services in enabling net-centric operations and to support interoperation across DoD. The operational concept should clearly state the DoD IEA Priority Areas, Principles, and Activities it has incorporated or addresses.

Technical federation, SOA, and technology innovation concepts describe additional means for enabling net-centric information sharing and operations. These means can be incorporated into an operational concept to complement the net-centric guidance provided by the DoD IEA. Based on the purpose, viewpoint, and scope of the architecture, the architect should select applicable elements from the descriptions of these concepts to direct the architecture's description of technical federation, SOA, and/or technology innovation in enabling net-centric operations and to support interoperation across DoD. By adding pertinent aspects of these concepts into the operational concept, the architect supplements the DoD IEA Priority Areas, Principles, and Rules, refining and extending them in defining operations and services able to address best practices for net-centric information sharing.

2.3.1.3.4 Align with JCA Taxonomy

Joint Capability Areas (JCAs) are “[c]ollections of like DoD capabilities functionally grouped to support capability analysis, strategy development, investment decision making, capability portfolio management, and capabilities-based force development and operational planning.”⁶ The Deputy Secretary of Defense has designated the JCAs for “immediate use as the Department's capability management language and framework.”⁷ **Table D-1** contains the definitions of the nine current tier 1 JCAs. Their definitions are the result of extensive collaboration among OSD, the Joint Staff, the Combatant Commands (COCOMs) and the

⁶ DoDD 7045.20, Capability Portfolio Management, September 25, 2008, p 8

⁷ DepSecDef Memo, Joint Capability Areas (JCAs), February 14, 2008

Combat Support Agencies. Under each tier 1 JCA is a hierarchy of capabilities grouped at tiers 2 and 3. Tiers 4 and 5 are presently under consideration for approval.⁸

Table D-1 - Tier 1 JCAs

JOINT CAPABILITY AREA	DESCRIPTION
Force Application	The ability to integrate the use of maneuver and engagement in all environments to create the effects necessary to achieve mission objectives.
Command & Control	The ability to exercise authority and direction by a properly designated commander or decision maker over assigned and attached forces and resources in the accomplishment of the mission.
Battlespace Awareness	The ability to understand dispositions and intentions as well as the characteristics and conditions of the operational environment that bear on national and military decision-making.
Net-Centric	The ability to provide a framework for full human and technical connectivity and interoperability that allows all DOD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and protects information from those who should not have it.
Building Partnerships	The ability to set the conditions for interaction with partner, competitor or adversary leaders, military forces, or relevant populations by developing and presenting information and conducting activities to affect their perceptions, will, behavior, and capabilities.
Protection	The ability to prevent/mitigate adverse effects of attacks on personnel (combatant/non-combatant) and physical assets of the United States, allies and friends.
Logistics	The ability to project and sustain a logistically ready joint force through the deliberate sharing of national and multi-national resources to effectively support operations, extend operational reach and provide the joint force commander the freedom of action necessary to meet mission objectives.
Force Support	The ability to establish, develop, maintain and manage a mission ready Total Force, and provide, operate, and maintain capable installation assets across the total force to ensure needed capabilities are available to support national security.
Corporate Management & Support	The ability to provide strategic senior level, enterprise-wide leadership, direction, coordination, and oversight through a chief management officer function (<i>Note: The Secretary of Defense currently assigns, in DoD Directive, the management duties and responsibilities for improving and evaluating overall economy, efficiency, and effectiveness to the Deputy Secretary of Defense</i>).

The Net-Centric JCA (highlighted in the table), provides high-level definitions of those enterprise capabilities that must be present for net-centric information sharing to occur. Although the Net-Centric JCA defines the primary capabilities required for net-centric information sharing, related capabilities enabling net-centric operations are defined by other JCAs, specifically Command & Control and Battlespace Awareness. To accurately define net-centric capabilities, language in the JCAs and the DoD IEA will align.

Architecture descriptions need to establish the net-centric characteristics their capabilities must exhibit to achieve the desired information sharing described in the net-centric operational concept. This requires the architecture context to first align with the JCA structure to provide the architect with those capabilities the architecture needs to describe. The intent is for the architect to then use the common capability terminology resulting from this alignment to locate requirements defined by the Capability Portfolios associated with the selected capabilities for use in describing capabilities in the architecture so they enable net-centric operations.

⁸ See JCA Taxonomy, found at http://www.dtic.mil/futurejointwarfare/cap_areas.htm

Determining which JCA capabilities should be incorporated into the architecture description to enable net-centric information sharing means first determining the applicable tier in the JCA structure, based on the architecture's stated purpose, viewpoint, and scope. Those capabilities which the architecture should address are then selected from the ones at that tier. Once this selection has been made, the JCA capabilities with which the architecture is to align should be included in the context description for the architecture. The context description should point out which JCA capabilities are to be described by the architecture and how they are to be addressed.

Properly incorporating net-centric capabilities from the JCAs in the context description requires answering the following questions for the architecture, based on the perspective it takes of the DoD IE:

- Will the architecture need to describe the provision of one or more of the capabilities from the identified JCA tier?
- Will the architecture need to describe the use of one or more of the capabilities from the identified JCA tier?

The architect uses the approved common language for the selected capabilities to select from architecture descriptions detailing JCA capabilities (e.g., the capability architectures for the various portfolios aligned with the JCAs) those net-centric attributes and requirements necessary for describing net-centric capabilities in the architecture, thus aligning the architecture description with JCA-defined capabilities. How the resulting capability characteristics and requirements are applied in the architecture description depends upon the perspective the architecture takes of the DoD IE:

- Where the architecture describes the provision of net-centric capabilities, the selected JCA capabilities should be used to locate those net-centric characteristics the capabilities defined by the architecture must exhibit.
- Where the architecture describes the use of net-centric capabilities, the selected JCA capabilities should be used to locate the net-centric characteristics of those capabilities available for access and consumption. The architecture description should then address how those characteristics are used in consuming the capability.

2.3.2 Align Architecture Description with DoD IEA

In this step, the architect uses the net-centric context established for the architecture to develop and maintain an architecture description aligned with the DoD IEA. How this alignment is accomplished varies according to whether the architecture is an enterprise (Department, capability, component) or a solution architecture.

2.3.2.1 Alignment for All Architectures

For all DoD architectures, the architect applies net-centric terms from the Net-Centric JCA taxonomy and the DoD net-centric strategy documents in the architecture description. Throughout the architecture life cycle, the architect should also be cognizant of, and use

where appropriate, any extensions to this net-centric vocabulary defined by Communities of Interest (COIs) in support of their problem spaces/domains.

The definitions of these terms should be applied in the architecture description so it properly represents net-centric attributes in aligning with the DoD Net-Centric Vision, as defined by the DoD IEA. Although it is not necessary to incorporate the definitions of these terms directly into the architecture description “word for word,” it is important for the architect to use these terms in a way that is consistent with the DoD IEA and its description of the net-centric DoD IE.

2.3.2.2 Alignment for Enterprise Architectures

For enterprise architectures, the architect applies Principles, Rules, and Activities from the DoD IEA in the architecture description to exhibit key net-centric attributes and guide the definition of capabilities and services to meet the requirements of the net-centric DoD IE. Department and capability architecture descriptions will primarily focus on aligning with the DoD IEA’s Principles and Rules. The high-level requirements of such architectures should be consistent with the high-level guidance articulated in Principles and Rules. At the same time, architects producing these architectures may find additional context and some details for the Principles and Rules in the higher level Activities in the DoD IEA Hierarchical Activity Model.⁹ Component architectures will also need to align with the DoD IEA’s Principles and Rules; however, the primary focus of Component EA alignment will be on DoD IEA Activities.

2.3.2.2.1 Incorporate Applicable DOD IEA Principles

The DoD Net-Centric Vision will be realized through adherence to DoD IEA Principles. The DoD IEA Principles are enduring guidelines describing ways in which an organization should operate to fulfill its mission. These Principles should be used to express an organization’s intentions so design and investment decisions can be made from a common basis of understanding.

At a minimum, all enterprise architecture descriptions need to account for the DoD IEA Global Principles and address the net-centric direction, guidelines, and scope they provide. Selecting the remaining Principles applicable to the architecture requires using the previous determination of applicable DoD IEA Priority Areas.

Each DoD IEA Priority Area has a related set of Principles.¹⁰ Once a Priority Area has been selected as applicable to the architecture and incorporated into its operational concept, the Principles it describes should be further assessed for their applicability based on the architecture’s purpose, viewpoint, and scope. All those Principles which fit should be applied

⁹ Located at the DoD IEA web site, http://www.defenselink.mil/cio-nii/sites/diea/DIEA_HTML/IWP/default.htm.

¹⁰ In addition, the CIR, CR, and NOA Priority Areas have been grouped in the DoD IEA document under Shared Infrastructure Environment (SI). The SI area has a set of Principles and Rules applicable to all three of its subordinate Priority Areas. These Principles and Rules should be considered whenever one or more of the SI components are selected as applicable to an architecture.

in the architecture description. How they are applied depends upon the perspective the architecture takes of the DoD IE:

- Where the architecture takes the provider and/or manager perspective, the applicable DoD IEA Principles should be applied directly to constrain descriptions of and provide guidelines for the development, delivery, and operation of DoD IE data and services.
- Where the architecture takes the consumer perspective, the applicable DoD IEA Principles should be applied indirectly to describe the amount and type of support the DoD IE can be expected to provide and to identify guidelines for accessing and using its data and services.

The DoD IEA Principles should be used in architecture descriptions to place restrictions or limitations on operations, providing bounds on how those operations are conducted. In addition to being placed in operational concepts, they could be expressed separately in the architecture description as guidelines or policy controlling the behavior of operational models. As such, they could be used in enterprise architecture descriptions as controls in activity models. They could also be incorporated into the definitions of operational activities to describe how those activities are to operate. Each architecture description should point out the DoD IEA Principles it has applied and identify where those Principles were applied.

2.3.2.2.2 Apply DoD IEA Rules

The DoD IEA Rules 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 enterprise architectures to ensure the resulting capability and service definitions reflect requirements from net-centric policies, guidance, and strategies.

The architect begins by determining which Rules are applicable to the architecture based on its purpose, viewpoint, and scope. The DoD IEA groups Rules under each of the Priority Areas, and in some cases (i.e., SA and NOA) under specific Principles in those Priority Areas. The architect can use these groupings to choose applicable Rules from those associated with the Priority Areas and/or Principles previously determined to be applicable to the architecture.¹¹

There are numerous ways to apply the DOD IEA Rules as constraints in an enterprise architecture description. The following paragraphs contain examples of three different approaches. However, these examples are not all inclusive and should not be considered the only valid solutions.

¹¹ In addition, the CIR, CR, and NOA Priority Areas have been grouped under a Shared Infrastructure Environment (SI) category. The SI area has a set of Principles and Rules applicable to all three of its subordinate Priority Areas. These Principles and Rules should be considered whenever one or more of the SI components are selected as applicable to an architecture.

- **Incorporate DoD IEA Rules into activity, process, and/or service definitions in the architecture description** – Selected DOD IEA Rule statements could be incorporated directly into the definitions of activities, processes, or services in the architecture description. In this way, the Rule statements become an integral part of the description of how an action, process, or service operates, limiting these descriptions to boundaries imposed by the 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 net-centric restrictions imposed by the DoD IEA, allowing the resulting capabilities to effectively operate in the DoD IE by meeting requirements from net-centric strategies, policy, and guidance.
- **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 net-centric 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 net-centric functionality and are capable of operating in the DoD IE. Since DoD IEA Rules primarily focus on providing an effective net-centric environment 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.

2.3.2.2.3 Align Operations and Processes with Related DoD IEA Activities

For component architectures, the architect also identifies DoD IEA Activities applicable to the architecture description, based on its purpose and scope. Applicable activities should be selected based on the DoD IEA Rules identified in the previous step as applicable to the architecture. The DoD IEA links Rules to Activities in the Activity decompositions associated with each Priority Area.¹²

¹² These links can be found in the Hierarchical Activity Model on the DoD IEA web site (http://www.defenselink.mil/cio-nii/sites/diea/DIEA_HTML/IWP/default.htm). Rules linked to an Activity can be located by clicking on an Activity box on the node tree in the diagram. When the definition screen appears, scroll down to see a list of linked Rules.

The list of DoD IEA Activities applicable to the architecture can be refined, extended, or reduced using the following complementary approaches:

- **Use the net-centric operational concept to identify applicable Activities.** Where high-level Activities from the DoD IEA have been used in developing the net-centric operational concept for the architecture, subordinate Activities could then be evaluated for their applicability to the architecture.
- **Identify Activities associated with applicable Priority Areas.** Each of the DoD IEA Priority Areas has an associated Activity decomposition. Based on the Priority Areas selected as applicable to the architecture, the architect could identify corresponding Activities from the associated decompositions to apply to the architecture.
- **Select Activities enabling technical federation, SOA, and technology innovation.** The supplemental concepts of technical federation, SOA, and technology innovation identified as being applicable to the architecture during development of the operational concept could also be used to determine DoD IEA Activities applicable to the architecture. Many of the DoD IEA Activities enable or support these concepts. For example, Activities can be found in the Hierarchical Activity Model¹³ for technical federation at A2(11) Provide for Federation, for SOA at A1 Provide Data and Services Deployment, and for technology innovation at A361 Advance Computing Infrastructure Technology.

How operational activities and processes in the architecture description align with the selected DoD IEA Activities depends on the perspective the architecture takes of the DoD IE:

- **Provider Perspective:** The DSD Priority Area contains activities applicable to the development of data and services in an SOA (A14 Provide Common End User Interfaces and A15 Develop Design Patterns for Data and Services) and so are a primary source for activities describing how required data and services in general are provided in the DoD IE. The DSD also includes activities describing the provision of specific enterprise services (A11 Provide Discovery Services, A12 Provide Core Enterprise Services, A13 Provide Collaboration Services, and A17 Enable Trust) to support user (including unanticipated user) needs. Specific Activities in the other Priority Areas also describe the provision of capabilities for those Priority Areas. For example, the Evolve Computing Infrastructure Activity (A36) subordinate to the CIR Priority Area contains subordinate activities for providing computing infrastructure.
- **Manager Perspective:** The NOA Priority Area is focused on managing and operating the DoD IE as a whole, and so is the primary source for Activities describing how capabilities are to be managed and operated to ensure the DoD IE is available and ready for use. In addition, the DSD, SA, CIR, and CR Priority Areas each contain specific Activities describing in particular how capabilities in each of these areas are to be managed and operated.

¹³ On the DoD IEA web site at http://www.defenselink.mil/cio-nii/sites/diea/DIEA_HTML/IWP/default.htm.

- **Consumer Perspective:** The Activities in the DSD Priority Area should be applied to architecture descriptions for defining how to use enterprise services in the DoD IE. The DSD Activities are also important for describing in the architecture those common guidelines governing use of any data and service available in the DoD IE. The SA Priority Area is an important source for Activities to use in describing the required access and authorization controls to be imposed on DoD IE users. Specific Activities in the other Priority Areas also describe how to access and use capabilities associated with each of these areas. Consequently, the descriptions for these Activities should be mined for guidelines and restrictions to be applied in the architecture to direct use of data and services provided by each of these other Priority Areas, as applicable.

The architect also needs to determine how to represent alignment with the applicable DoD IEA Activities. This representation depends upon the perspective the architecture takes of the DoD IE in regards to the activity or process being aligned. Where the architecture is describing the provider or manager perspective, the pertinent operational activities and processes in the architecture description should be directly derived from the 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 DoD IE data and services, the architect needs to relate applicable DoD IEA Activities to operational activities and processes in the architecture description to show how architecture 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 subprocesses 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 DoD IE.

2.3.2.3 Alignment for Solution Architectures

For solution architecture descriptions, the architect needs to first align with the net-centric attributes and requirements contained in those higher level enterprise architectures governing the solution space. The architect would then select and add applicable leaf-level Activities and associated relevant Constraints and Mechanisms from the DoD IEA to the solution architecture description where gaps in enterprise architecture guidance exist and/or to further refine the solution description.

2.3.2.3.1 Align with Applicable Enterprise Architecture Descriptions

Solution architectures should be derived from and governed by higher level capability and component architectures. In accordance with the previous subsection describing DoD IEA alignment for enterprise architectures, net-centric enterprise architecture descriptions will be aligned with the DoD IEA by incorporating, as applicable, its Principles, Rules, and Activities in describing interactions with the DoD IE. Such net-centric enterprise architecture descriptions will then refine, extend, and enhance these applicable DoD IEA elements to describe in greater detail requirements for interacting with the net-centric DoD IE in their domains. Each solution architecture description should be first aligned with the net-centric elements in the applicable enterprise architecture descriptions. The solution architecture descriptions should incorporate the associated net-centric requirements from these higher level architecture descriptions as starting points in describing the required solution space. In this way, the solution architecture description is properly aligned with the DoD IEA through alignment with the appropriate governing enterprise architecture descriptions.

2.3.2.3.2 Incorporate Leaf-Level DoD IEA Activities

In some cases, higher level enterprise architecture descriptions may not provide a complete set of net-centric requirements or the level of detail necessary for completely defining the solution's interaction with the DoD IE. In these situations, the solution architect may need to align the solution architecture description with additional material from the DoD IEA. The architect would begin this process by determining additional leaf-level DoD IEA Activities¹⁴ applicable to the required solution. Depending upon the architecture's purpose, viewpoint, and scope, and its perspectives of the DoD IE, such Activities should be used in describing how the solution is to be provided and/or managed/operated to supply the desired net-centric capability or how it is to use the DoD IE to enable net-centric operations, in line with restrictions and constraints imposed by applicable higher level enterprise architecture descriptions. The selected leaf-level DoD IEA Activities would primarily be used as starting points for activity or function decompositions to provide more detailed descriptions of how a solution operates in the net-centric DoD IE. Applicable leaf-level Activities should be selected based on the DoD IEA Priority Areas, Principles, and Rules with which the enterprise architecture descriptions superior to the solution architecture have been aligned.

¹⁴ Leaf-level activities are those found at the lowest level in the Hierarchical Activity Decomposition.

2.3.2.3.3 *Apply DoD IEA Constraints and Mechanisms*

In the DoD IEA, Constraints and Mechanisms have been defined and linked to leaf-level DoD IEA Activities.¹⁵ In the DoD IEA, Constraints and Mechanisms provide practical guidance for implementing Activities and complying with Rules. The Constraints are generally references to strategic documents or DoD Directives; however, there are Constraints that are working groups, websites, and other “resources” that control an Activity. The Mechanisms, on the other hand, are generally “tools” that provide additional detail on the way a requirement might be accomplished. The DoD IEA Mechanisms are examples, not necessarily the only way the requirement could be accomplished. Programs align with the DoD IEA by complying with the applicable Constraints. They could use the applicable Mechanisms to accomplish this compliance.

By incorporating into a solution architecture description appropriate Constraints and Mechanisms linked to leaf-level DoD IEA Activities selected as applicable in the previous step, the architect can shape the architecture description so it further aligns with the DoD IEA by incorporating net-centric attributes and requirements defined by these Constraints and Mechanisms. Constraints and Mechanisms must be applied so they are consistent with the Principles, Rules, and Activities applicable to the solution, as determined by those enterprise architectures that guide or direct the solution.

2.3.3 Support Architecture Use

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

For all these architectures, the architect works with users to analyze the architecture in answering 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 viewpoint and scope and stakeholder needs. However, a general list of pertinent net-centric-related questions is provided in Appendix E Compliance with the DoD IEA.

¹⁵ To locate these Constraints and Mechanisms, use the Hierarchical Activity Model on the DoD IEA web site (http://www.defenselink.mil/cio-nii/sites/diea/DIEA_HTML/IWP/default.htm). Click on an Activity box in the node tree. When the definition screen for the Activity appears, scroll down to see a list of Constraints and a list of Mechanisms associated with the Activity.

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 net-centric data and services to meet mission needs.

2.3.3.1 Analyze Architecture

This process begins with the conduct of an analysis of the contents of a net-centric architecture 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 must be involved prior to architecture development in defining the types of analyses required and the information those analyses must provide.¹⁶ 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. How architecture users apply the results of these analyses is described in more detail in subsequent sections. 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 net-centric goals and objectives. The net-centric 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 initiatives and programs for actually filling identified gaps and correcting identified redundancies and dead-ends, enabling architecture requirements and meeting critical mission needs.
- **Management Analysis** involves use of the architecture description in developing more detailed guidelines for use in managing investments and programs to meet net-centric goals and objectives and, most importantly, follow net-centric policy. 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

¹⁶ This information is then used in planning the architecture and its development and should be captured in its overview and summary information.

in directing portfolios and programs and as the basis for selecting solutions to meet established needs.

2.3.3.2 Support Use of Architecture

The architect then works with architecture stakeholders to support proper use of the architecture and architecture analyses in achieving required net-centric capabilities. Once properly aligned with the DoD IEA (per the preceding process), the architecture contains the Principles, Rules, and Activities for aligning portfolios and/or programs to the DoD IEA to meet net-centric policy and guidance. Because of the importance of investment and program management use of architectures, the next two sections focus on how a net-centric architecture, aligned with the DoD IEA, could be used to enable the actions of PEOs/PMs and decision-makers, to include CPMs and IRBs.

3. Application of DoD IEA in Program Management

This section describes how PEOs/PMs could use solution architectures, properly aligned with the DoD IEA, in carrying out their responsibilities. Program Executive Officers and PMs in the Components are the designated individuals with responsibility for and authority to accomplish objectives for program development, production, and sustainment to meet users' operational needs.¹⁷ In particular, PMs are a focal point for providing decision-makers with information on Programs of Record (PoRs) and how these PoRs meet net-centric information sharing requirements. As such, PMs are responsible for ensuring that all required data on their PoRs provide an accurate picture of the state of the program, in the context of the DoD IE, to enable their Component organizations, as well as DoD CPMs, IRBs, the CIO, and the Defense Business Systems Management Committee (DBSMC), to make informed decisions.¹⁸

Figure D-5, Example of PEO/PM Use of DoD IEA, shows how the PEO/PM might use a net-centric solution architecture, aligned with the DoD IEA, to support program design and implementation.

¹⁷ The Defense Acquisition System, DODD 5000.1, May 12, 2003

¹⁸ Business Transformation Agency, DoD IT business Systems Investment Review Process, Investment Certification and Annual Review Process User Guide, 10 April 2006.

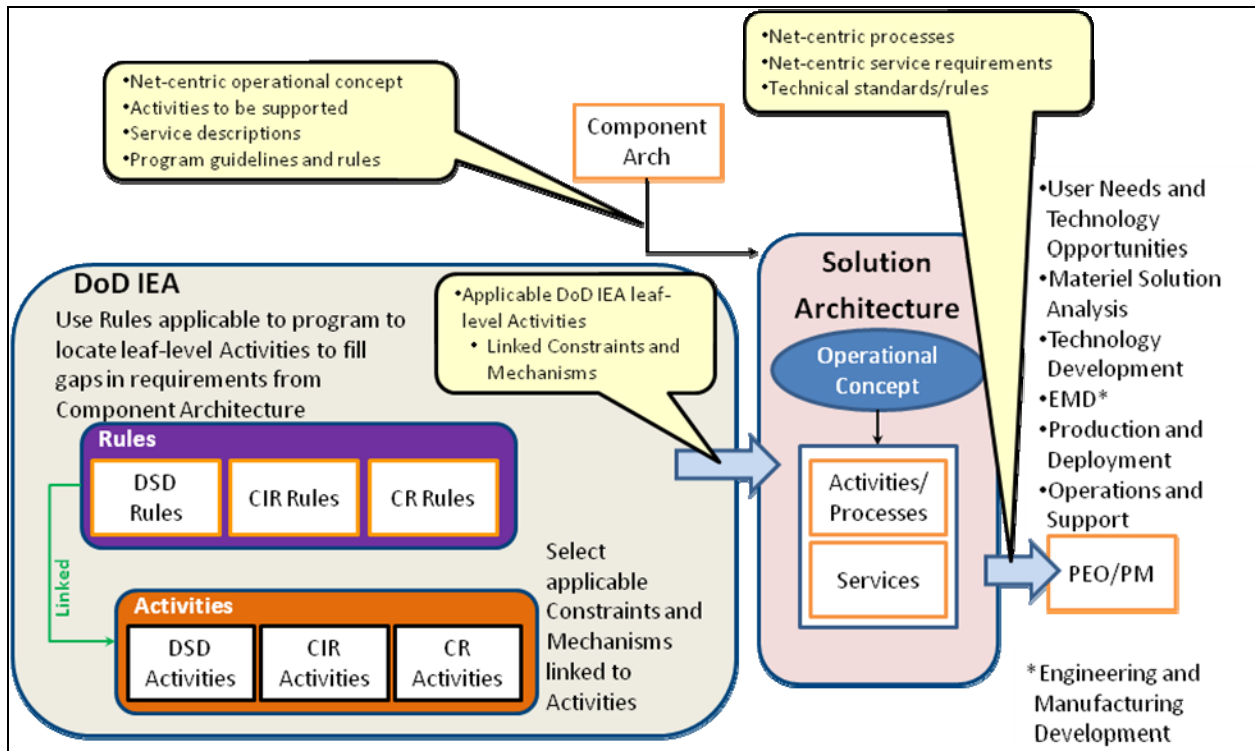


Figure D-5 - Example of PEO/PM Use of DoD IEA

The solution architecture for the program should be derived from and compliant with appropriate higher-level component architectures. These component architectures provide the solution architect with an operational concept the program must follow, a set of higher level activities the program must support, descriptions of required services the program is to provide, and additional guidelines to which the program must adhere. The applicable component architectures are assumed to have been aligned with the DoD IEA to properly capture the net-centric aspects of the domain or space the component architecture is addressing and to be conformant with the net-centric aspects of more senior enterprise architectures and Department guidance.

In developing the solution architecture, the architect has taken into consideration DoD IEA Priority Areas, Principles and Rules, and Activities as applied by governing component architecture(s). The DoD IEA Rules applicable to the solution have been used to determine additional leaf-level DoD IEA Activities the solution must provide or support. The architect has incorporated these Activities into the solution architecture in accordance with the perspective the solution takes of the DoD IE (provider, manager, and/or consumer of data and services). The applicable DoD IEA Rules further constrain those net-centric capability attributes and requirements from capability and component architectures applicable to the solution architecture description. The PEO/PM can use the net-centric operational processes, service requirements, and rules from the solution architecture to manage the program and select solutions to meet program needs by deriving non-functional requirements, design criteria and guidelines, and criteria for analyzing alternatives.

The PEO/PM should also incorporate specific DoD IEA Constraints and Mechanisms into solution design and evaluation to ensure the resulting service(s) meet DoD IEA requirements.¹⁹ The DoD IEA Constraints provide external requirements to which the resulting programs must adhere. The DoD IEA Mechanisms provide examples of effective solutions for meeting net-centric requirements. The PEO/PM, in conjunction with the solution architect, determines the Constraints and Mechanisms applicable to the program based on the DoD IEA leaf-level Activities the solution is to execute and/or support.

In addition, the architect can assist the PEO/PM in using the concepts of technical federation, SOA, and technology innovation to establish unique design and evaluation criteria related to specific aspects of these best practices with particular application to the PoR:

- The elements of technical federation could be used to define criteria for determining if solution options will be able to operate in a federated environment
- Criteria could be derived from the SOA concept to evaluate if potential solutions can act in a service oriented environment (e.g., are the proposed solutions truly services, can the proposed solutions interoperate with services, etc.)
- The technology families enabling net-centric information sharing from technology innovation could be used to derive criteria to determine if these technologies are or should be incorporated in a solution to achieve net-centric requirements

The appropriate timeframe to start implementing DoD IEA guidance on net-centric information sharing and associated program interoperability is during the Capabilities Based Assessment (CBA) phase of the JCIDS process.²⁰ The CBA sets the stage for subsequent acquisition. Before initiating a program, the CBA identifies warfighting capability and supportability gaps and the Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, and Facilities (DOTMLPF) capabilities 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 net-centric capabilities to fill the identified gaps. Because the Joint Capabilities Document (JCD) or Initial Capabilities Document (ICD) developed during the CBA provides the formal communication of capability needs between the warfighter, acquisition, and resource management communities, it must incorporate appropriate DoD IEA elements in defining the net-centric 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

¹⁹ To locate the Constraints and Mechanisms, use the Hierarchical Activity Model on the DoD IEA web site (http://www.defenselink.mil/cio-nii/sites/diea/DIEA_HTML/IWP/default.htm). Click on a leaf-level Activity box in the node tree. When the definition screen for the Activity appears, scroll down to see a list of Constraints and a list of Mechanisms associated with that Activity.

²⁰ CJCSI 3170.01F, 1 May 2007

and system requirements, and the maturation of technologies that lead to disciplined development and production of systems that provide increasing capability over time.²¹

In support of evolutionary acquisition, DoD IEA Priority Areas, as applied to higher level capability and component architectures, describe transformation priorities the PEO/PM can use to determine which initial capabilities should be developed and/or acquired. The common net-centric vision described by the DoD IEA, as incorporated into the applicable solution architecture(s), with additional detail provided by the descriptions of applicable net-centric capabilities from higher level capability and component architectures, can also be used to determine the required end-state of net-centric capabilities to be provided by the program. The DoD IEA Principles and Rules, as applied in capability and component architectures, can be used to establish criteria for assessing the current position of the program in meeting net-centric requirements and for planning future improvements and defining incremental development goals to address requirement gaps.

The PEO/PM must ensure the programs for which they are responsible comply with all DAS directives and instructions. The remaining subsections describe program management responsibilities associated with specific phases of the DAS process, as defined in DoDI 5000.02. The subsections describe how a PEO/PM can use architectures, aligned with the DoD IEA, to filter applicable laws, regulations, policies, standards, and frameworks and fulfill program management responsibilities associated with each of these phases.

3.1 User Needs and Technology Opportunities

The capability needs and acquisition management systems use Joint Concepts, integrated architectures, and an analysis of DOTMLPF in an integrated, collaborative process to define needed capabilities to guide the development of affordable systems. Representatives from multiple DoD communities assist in formulating broad, time-phased, operational goals, and describing requisite capabilities in an Initial Capabilities Document (ICD). They examine multiple concepts to optimize the way DoD provides these capabilities.²²

As part of this process, the PM must collaborate with other PM's, Services, and DoD Agencies to develop a solution architecture integrated with architectures of other programs, as well as with the overall Department vision. For designated programs, the PEO/PM is required to present a solution architecture using the DoDAF to demonstrate how the program fits with Joint Architectures derived from applicable Joint Strategies. Furthermore for all programs, the program is required to comply with DoD IA Directives, interoperability requirements, and spectrum management requirements associated with net-centric operations support.

The DoD IEA Priority Areas, Principles, Rules, and Activities provide a common understanding of net-centric concepts to facilitate collaboration among PMs. The standard language for net-centric information sharing in the DoD IEA can be used to integrate solution architectures and for developing measures to determine alignment of programs with the DoD Net-Centric Vision. Since the DoD IEA unifies the Department's Net-Centric Strategies,

²¹ DoDI 5000.02, Dec 2, 2008, p. 13

²² DoDI 5000.02, Dec 2, 2008, p. 14

policy, and guidance, the PEO/PM can use a solution architecture aligned with the DoD IEA as previously described to direct resulting programs in complying with this policy. Aligning solution architectures with the DoD IEA provides a net-centric basis for these architecture descriptions, demonstrating how the program fits with joint architectures derived from the net-centric strategies. The DoD IEA and aligned component architectures provide the PEO/PM with an integrated set of Activities for achieving information assurance, service orientation, and data sharing in enabling net-centric operations in support of interoperation across DoD.

3.2 *Materiel Solution Analysis*

The purpose of this phase is to assess potential materiel solutions and to satisfy the phase-specific entrance criteria for the next program milestone designated by the Milestone Decision Authority (MDA). The designated lead DoD Component(s) prepares an Analysis of Alternatives (AoA) study plan to assess preliminary materiel solutions, identify key technologies, and estimate life-cycle costs. The purpose of the AoA is to assess the potential materiel solutions to satisfy the capability need documented in the approved ICD. The AoA focuses on identification and analysis of alternatives, measures of effectiveness, cost, schedule, concepts of operations, and overall risk. The AoA assesses the critical technology elements (CTEs) associated with each proposed materiel solution, including technology maturity, integration risk, manufacturing feasibility, and, where necessary, technology maturation and demonstration needs. To achieve the best possible system solution, emphasis is placed on innovation and competition. Existing commercial-off-the-shelf (COTS) functionality and solutions drawn from a diversified range of large and small businesses are considered.²³

A solution architecture, properly aligned with the DoD IEA, provides the basis for the criteria used by a PM to conduct an AoA. The solution architecture should contain net-centric rules derived from applicable Rules in the DoD IEA to provide net-centric attributes and requirements the program must meet in order to properly operate in the target DoD IE. These technical rules should be used in developing criteria to measure how well a proposed solution addresses such requirements. The leaf-level DoD IEA Activities applied to the solution architecture describe the actions solutions must take to meet applicable DoD IEA Rules; criteria related to such Rules can be used to determine if alternatives provide the proper functionality. Finally, related Constraints and Mechanisms from the DoD IEA, applied to a solution architecture, provide a basis for assessing solution alternatives; Constraints are additional restrictions and requirements the solution must meet, while Mechanisms describe actual examples meeting net-centric requirements to which alternatives can be compared.

3.3 *Technology Development*

The purpose of Technology Development is to reduce technology risk and determine the appropriate set of technologies to be integrated into the service to be delivered by the program. Technology Development is a continuous technology discovery and development

²³ DoDI 5000.02, Dec 2, 2008, p. 15

process, reflecting close collaboration between the scientific and technical (S&T) community, the user, and available technologies, all while simultaneously refining user requirements.²⁴

The PEO/PM can use the solution architecture, as aligned with higher level capability and component architectures and the DoD IEA, in selecting and integrating technologies into a program. A net-centric solution architecture provides the PEO/PM with net-centric guidance, Constraints and Mechanisms, and standards for net-centric information sharing for specifying and evaluating target technologies. Potential net-centric target technologies may be selected from technology families derived using the technology innovation concept and from Mechanisms linked to applicable leaf-level DoD IEA Activities. Such technologies may be determined using the solution architecture's description of the net-centric vision for the program's interaction with the "to be" DoD IE to establish technology requirements for specified net-centric capabilities. By determining which technologies are necessary drivers for the net-centric evolution of the DoD IE and the services using it, the PEO/PM can establish priority lists of technologies for inclusion in programs and can assess solutions for their ability to provide such technologies. As target technologies mature, they can be compared to applicable Constraints and Mechanisms to determine if the technologies can provide the desired net-centric capabilities and so enable net-centric material solutions.

3.4 Engineering and Manufacturing Development (EMD)

The purpose of the EMD phase is to develop a system or an increment of capability; complete system integration (technology risk reduction occurs during Technology Development); develop an affordable and executable manufacturing process; ensure operational supportability with particular attention to minimizing the logistics footprint; implement human systems integration (HSI); design for producibility; ensure affordability; protect critical program information CPI by implementing appropriate techniques such as anti-tamper; and demonstrate system integration, interoperability, safety, and utility. The Capability Development Document (CDD), Acquisition Strategy, Systems Engineering Plan (SEP), and Test and Evaluation Master Plan (TEMP) guide this effort.²⁵

During EMD, a net-centric solution architecture, aligned with applicable higher level capability and component architectures and the DoD IEA, can provide the detailed description of the net-centric environment for determining and demonstrating required functionality for net-centric operations and system interoperation. The applicable DoD IEA Constraints and Mechanisms will direct net-centric functions and establish net-centric requirements, giving the PEO/PM the tools to design a service capable of delivering the needed net-centric capability in the "to be" DoD IE. The descriptions of applicable leaf-level DoD IEA Activities can be used to determine the net-centric operations the service must support and can guide definition of the necessary functions and selection of technology families to incorporate into services. The DoD IEA Activities also describe how services should be developed so they can operate properly and effectively in the DoD IE and provide context for use in simulating DoD IE support during demonstrations and tests. The applicable DoD IEA Activities, Constraints, and Mechanisms, combined with descriptions of attributes and

²⁴ DoDI 5000.02, Dec 2, 2008, p.16

²⁵ DoDI 5000.02, Dec 2, 2008, p. 20

requirements of applicable net-centric capabilities, provide a basis for developing criteria to use in testing the net-centric aspects of a service.

A net-centric solution architecture, aligned with applicable higher level capability and component architectures and the DoD IEA, also provides the PEO/PM with a description of how subsystems should operate together and with the shared infrastructure in the DoD IE in support of net-centric operations to guide integration in achieving net-centric goals. The DoD IEA Constraints, combined with net-centric technical rules applicable to the program and requirements associated with applicable net-centric capabilities from supporting capability and component architectures, should be incorporated into the CDD to guide the integration of proper net-centric components into the service. The DoD IEA Constraints and net-centric rules applicable to the program in particular provide guidelines for integration so the service can meet net-centric requirements and operate in the “to be” DoD IE. The Constraints and rules should be applied to any prototype or EDM developed to demonstrate net-centric aspects of the integrated service.

3.5 Production and Deployment

The purpose of Production and Deployment is to achieve an operational capability satisfying mission needs. Operational test and evaluation conducted during this phase determines the effectiveness and suitability of the developed service for production or acquisition. The MDA decides whether to commit DoD to production or acquisition at Milestone C. Milestone C authorizes entry of Major Defense Acquisition Programs (MDAPs) and major systems into Low Rate Initial Production (LRIP), non-major systems not requiring LRIP into production or procurement, or Major Automated Information Systems (MAIS) programs or software-intensive systems with no production components into limited deployment in support of operational testing.²⁶

The leaf-level DoD IEA Activities applicable to the solution architecture should be used to develop criteria for Operational Test and Evaluation (OT&E) to assess whether the program can meet net-centric goals and operate effectively in the “to be” DoD IE. As a key aspect of the Milestone C determination, the MDA will also need to evaluate the net-centric elements of the program to determine its ability to meet net-centric requirements, as defined by the DoD Net-Centric Strategies. The applicable DoD IEA Constraints and Mechanisms, supplemented by descriptions of attributes and requirements for net-centric capabilities from supporting capability and component architectures, provide a basis for development of criteria to make this determination.

3.6 Operations and Support

Operations and Support has two major efforts: Sustainment and Disposal. The objective of Sustainment is the execution of a support program to meet operational support performance requirements and maintain the service in the most cost-effective manner over its total life cycle. When the service has reached the end of its useful life, it is then disposed of in an appropriate manner.²⁷

²⁶ DoDI 5000.02, Dec 2, 2008, p. 26

²⁷ DoDI 5000.02, Dec 2, 2008, p. 28

During the system lifecycle, the common vision of the net-centric environment provided by the solution architecture, as aligned with applicable higher level capability and component architectures and the DoD IEA, can be used as a baseline against which to assess how well the program is meeting net-centric requirements and for determining incremental changes to the system needed to address recognized shortfalls in net-centric functionality. The leaf-level DoD IEA Activities and associated Constraints and Mechanisms can also be used in making decisions regarding whether or not a service is operating to effectively support net-centric operations and for planning changes to bring service operation in line with net-centric goals. Net-centric criteria can further be developed from the DoD IEA Constraints and Mechanisms to use in determining when a service is no longer meeting the net-centric realities of the DoD IE and so should be replaced (i.e., disposed of).

4. Application of DOD IEA in Decision-Making

This section currently addresses only decision-making associated with IT investment management. Future versions of this Appendix may expand upon this description to address the application of DoD IEA to decision-making for other functions or processes.

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 Portfolio Management (PfM) process uses integrated strategic planning, integrated architectures, measures of performance, risk management techniques, transition plans, and portfolio investment strategies to manage selected groupings of IT investments. The Investment Review process complements and supports PfM by certifying business system modernizations in excess of \$1 million over the system modernization lifecycle and directing DoD Components in the conduct of annual reviews of business system investments. The following subsections describe how the DoD IEA Principles, Rules, and Activities, as applied to supporting architectures, can provide CPMs and IRBs with the means to make informed decisions regarding IT investments.

4.1 Portfolio Manager Use of DoD IEA

Proper execution of PfM requires portfolio managers to have the information necessary to make informed decisions regarding investments in net-centric capabilities. Architects and PEOs/PMs provide the portfolio manager with this information. Consequently, to achieve net-centric transformation, both architects and PMs must properly align their products with the DoD IEA to provide the necessary information to make informed decisions regarding investments in required net-centric capabilities. **Figure D-6**, Example of CPM Use of DoD IEA, shows how a net-centric capability architecture, aligned with the DoD IEA, could be used by a CPM in making investment decisions to enable net-centric operations.

In developing a net-centric capability architecture, the architect has incorporated descriptions of DoD IEA Priority Areas, Principles, and applicable high-level Activities into a net-centric operational concept and has applied DoD IEA Principles to the description of capability operations in the architecture. The architect has aligned the architecture description with the

JCAs and has used the JCA taxonomy to locate and use appropriate net-centric attributes and requirements in shaping definitions of architecture capabilities so they are net-centric.

The architect can now assist the portfolio manager in applying the resulting net-centric assumptions, operational concept, and capability descriptions to guide investment determinations for the portfolio. The architect can support the portfolio manager in constructing criteria for use in making investment decisions by interpreting guidelines from DoD IEA Priority Area descriptions, Principles, and high-level Activities, and net-centric capability requirements described in the capability architecture. The architect should also work with the portfolio manager to conduct a gap analysis to determine priority issues to address in the portfolio, as well as a management analysis to establish more detailed net-centric guidelines for use in managing the portfolio.

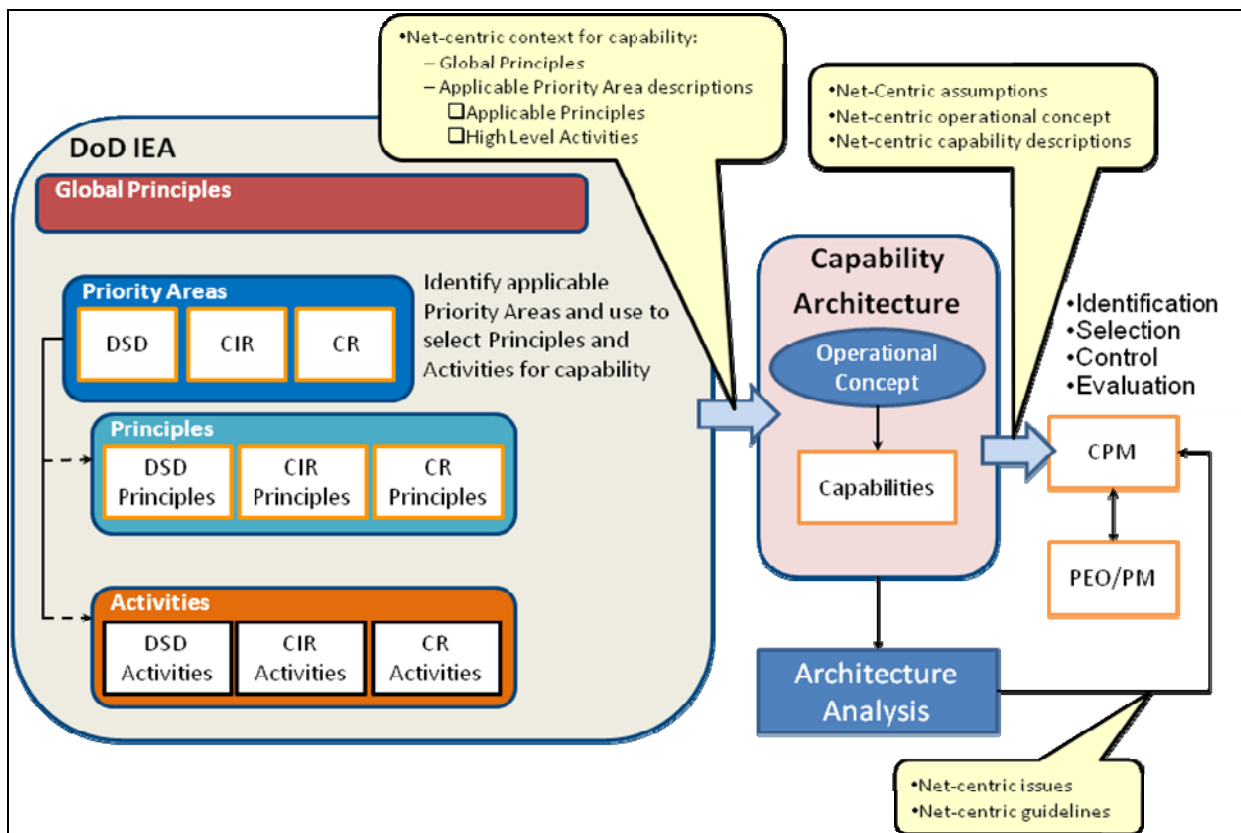


Figure D-6 - Example of CPM Use of DoD IEA

Portfolio management involves the identification, selection, control, and evaluation of information resources.²⁸ The next subsections describe the use of a net-centric capability architecture, aligned with the DoD IEA, to enable each of these functions.

²⁸ OMB Circular A-130, defines the capital planning and investment control process (CPIC) as a “management process for on-going identification, selection, control, and evaluation of investments in information resources.” DoD Directive (DoDD) 8115.01, Information Technology Portfolio Management, October 10, 2005, addressed four similar functions for portfolio management: Analysis, Selection, Control, and Evaluation.

4.1.1 Identification

In identification, the scope of the portfolio and the investments it should contain 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:

- 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

Since the DoD IEA synthesizes and integrates the DoD Net-Centric Vision, strategies, policies, and guidance, the portfolio manager can use a net-centric capability architecture aligned with the DoD IEA to provide the portfolio with objectives reflecting the Department's net-centric requirements. The DoD IEA Principles, as well as the descriptions of Priority Areas applicable to the architecture provide guidelines for the capabilities the portfolio must develop and support to achieve the Net-Centric Vision. Since the DoD IEA also unifies the goals and objectives of the DoD Net-Centric Strategies, it allows the construction of objectives aligned with these strategies. Each portfolio manager should focus investment planning toward providing the net-centric capabilities aligned with the applicable Priority Areas, as these Priority Areas represent key needs for transforming the DoD IE to its target state.

The portfolio manager can use the DoD IEA Principles and associated Rules incorporated into the capability architecture as a starting point for developing net-centric criteria for investment decision-making and to establish performance measures for tracking and grading those decisions. The portfolio manager can use these criteria to assess the portfolio baseline to determine net-centric capability gaps, opportunities, and redundancies. A portfolio manager could further use the descriptions of net-centric capabilities, as described in supporting capability 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).

In determining proper IT investment strategies, the portfolio manager should supplement the common vision of a net-centric DoD IE, as described in the supporting capability architecture, with additional net-centric context from the publications of the CCRP, the NCOE documents, and the net-centric enabling concepts of technical federation, SOA, and technology innovation. This additional information can help the portfolio manager to better understand and use the DoD IEA Principles and Rules. It provides supplemental net-centric attributes for determining the current state of net-centric investments in the portfolio, assessing gaps and redundancies in and priorities for net-centric capabilities, and establishing criteria to measure investments and investment risk against net-centric requirements. For example, technology

innovation can identify emerging net-centric technologies to be incorporated into the portfolio while pointing to the means for co-evolving technical characteristics of the portfolio with net-centric operational updates. Technology innovation also provides a basis for identifying risks associated with emerging technology and for further assessing technology gaps, opportunities, and redundancies in the portfolio.

4.1.2 Selection

During selection, the portfolio manager identifies and selects the best mix of IT investments to achieve the portfolio's goals and objectives, while demonstrating the impact of alternative IT investment strategies and funding levels on the portfolio. The DoD IEA provides a common language and context for the net-centric components of the DoD IE, as well as a basis for determining the full set of DOTMLPF attributes to review in evaluating potential net-centric capabilities. Use of the key net-centric terms contained in the DoD IEA, applied in the pertinent capability architectures, allows the portfolio manager to identify, compare, and evaluate the net-centric aspects of very different capability investments to judge their ability to enable net-centric information sharing.

As part of selection, the portfolio manager measures potential solutions against criteria derived during identification to establish whether those solutions should be part of the portfolio investments. Pros and cons can be identified for each solution based on its ability to meet the applicable DoD IEA Principles and Rules, address net-centric concepts, and provide required net-centric capabilities as described in the capability architecture. These measurements provide the data for adjusting the portfolio so it provides the best mix of investments to enable net-centric information sharing and implement the right solutions to meet net-centric 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 monitored and 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 DoD IEA Principles and Rules, as applied in the capability architecture, to determine whether programs can be expected to meet net-centric requirements and provide necessary net-centric capabilities. The portfolio manager also uses the net-centric enabling concepts of technical federation, SOA, and technology innovation to judge whether or not current investments can supply best practices in a net-centric DoD IE. The descriptions of applicable net-centric capabilities from the supporting capability 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 net-centric capability architecture.

4.1.4 Evaluation

Periodically, the portfolio manager measures the actual contributions of fielded capabilities provided by the portfolio to the enablement of net-centric operations. The portfolio manager measures the actual support provided by the portfolio 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 begin the identification function again.

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

4.2 *Investment Review Board Use of DoD IEA*

The Investment Review process was established to meet directives in the Ronald W. Reagan National Defense Authorization Act of Fiscal Year 2005 (FY05 NDAA). The FY05 NDAA mandated certification of DoD business systems modernization programs costing in excess of \$1 million over the course of the program or designated as Principal Staff Assistant (PSA) Interest Programs. In addition, the FY05 NDAA directed a periodic, but not less than annual, review of all DoD business system investments, regardless of cost and even if these systems are not undergoing current development or modernization.

To meet these directives, the DoD Business Transformation Agency (BTA) developed an IRB Concept of Operations (CONOPS) including a governance structure, roles, responsibilities, and processes for conducting the necessary business system certification and annual reviews.

²⁹ For the purposes of this discussion, this CONOPS is considered the de facto standard for IRBs across the Department.

Each of the DoD Components identifies the programs under its control requiring certification. The PMs for these programs are responsible for assembling certification packages containing accurate and complete information on their programs. Pre-Certification Authorities (PCAs), appointed by the Components, review and validate the certification packages, then submit them to the appropriate IRBs for certification review and recommendation. The IRBs submit programs they recommend for certification to designated Certification Authorities (CAs) at the Principal Staff Assistant (PSA) level. If the CA certifies a program, it is submitted to the

²⁹ Description of the IRB process in this section is taken from DoD IT Business Systems Investment Review Process, Investment Review Board Concept of Operations, July 12, 2006

Defense Business Systems Modernization Committee (DBSMC) for final approval and subsequent obligation of funds.

The DoD CIO is the CA for business systems supporting IT infrastructure or information assurance (IA), as described by Title 10 U.S.C., Section 222, subsection (f)(4).³⁰ Since the DoD IEA integrates key DoD strategies, policies, and guidance for achieving net-centric information sharing, its common vision of a net-centric DoD IE will be the foundation for developing certification criteria to be used by the DoD CIO in making decisions regarding these infrastructure and IA investments. However, the DoD IEA can also be used to locate commonalities in net-centric processes and services across all investments or programs for use in eliminating redundancies and promoting reuse of net-centric programs across the Department. Since the DoD IEA is aligned with the DoD strategic vision for transformation of the DoD IE to its target net-centric state, it can be used to determine if any investment or program is advancing towards the Department's common net-centric goals and so is aligned with DoD's needs in regards to net-centric operations.

Figure D-7, Example of DoD IEA Use in Certifying Investments, shows how an IRB might use the DoD IEA to determine whether an investment or program is compliant with DoD's Net-Centric Vision and associated requirements.

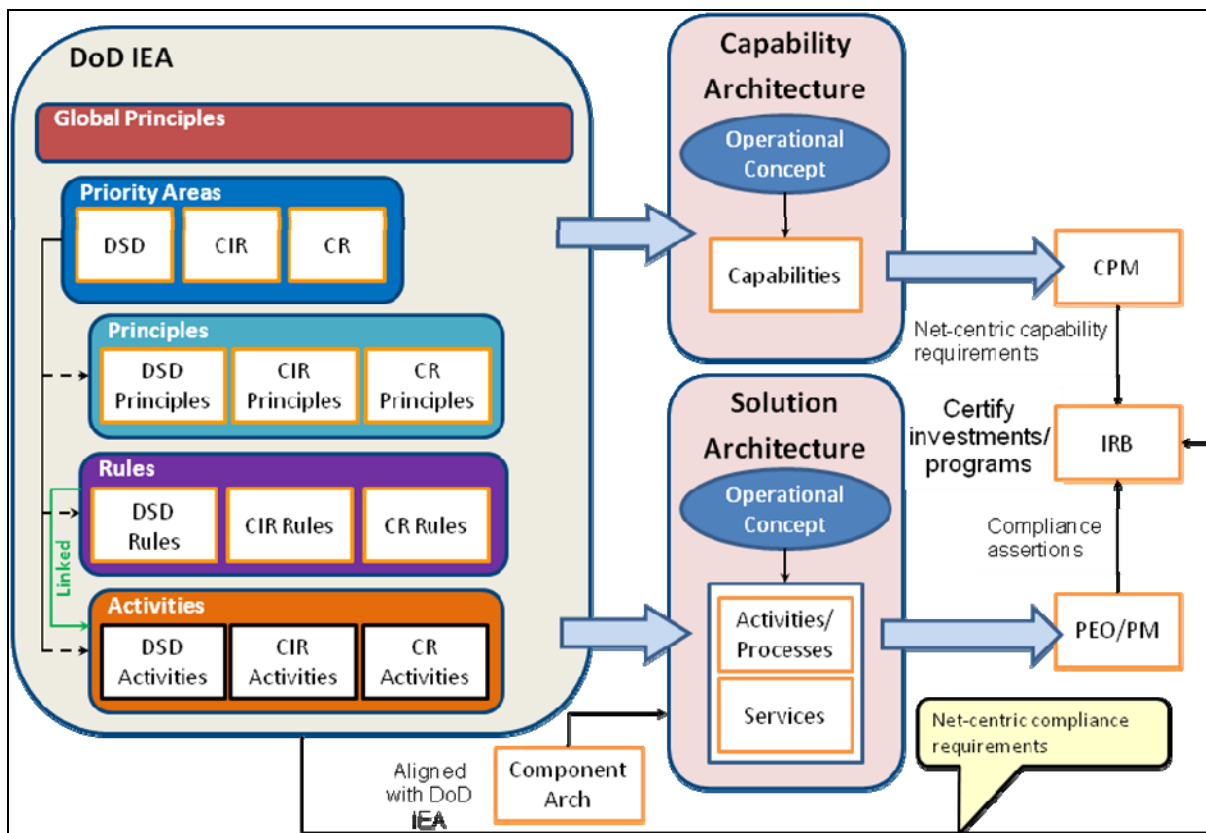


Figure D-7 - Example of DoD IEA Use in Certifying Investments

³⁰ DoD CIO IT Investment Review Board Compliance Certification Process, August 26, 2008, p. 2

To properly conduct a net-centric assessment of an investment or program, the IRB would need to receive information from both CPMs and PEOs/PMs with a stake in the investment or program under review. From CPM(s), the IRB would receive net-centric capability requirements associated with the portfolio. This information would be drawn from associated capability architectures aligned with the DoD IEA. As previously described, aligning capability architectures with the DoD IEA requires the architect to incorporate descriptions of applicable DoD IEA Priority Areas, associated Principles, and related high-level Activities into a net-centric operational concept for the capability and to align its operations and enabling service descriptions to applicable DoD IEA Rules and linked Activities. The architect must also align capability descriptions to the JCA taxonomy and use this alignment to locate net-centric attributes and requirements for shaping definitions of net-centric capabilities. In this way, the architect has incorporated DoD IEA guidelines into the capability architecture to direct investments or programs so they follow net-centric policy. The IRB can, therefore, assess compliance of the investment or program against the resulting net-centric capability requirements to determine if it aligns with DoD net-centric goals and objectives.

From PEO(s)/PM(s), the IRB would receive assertions as to how a program complies with net-centric requirements of the Department. These assertions are based on how the solution architecture(s) governing the program align with the DoD IEA. The solution architect first aligns with governing component architectures aligned to the DoD IEA, incorporating applicable DoD IEA Principles, Rules, and Activities as interpreted by these component architecture(s). The solution architect also incorporates additional leaf-level DoD IEA Activities and associated Constraints and Mechanisms into the solution architecture description in defining solution requirements and providing detailed technical standards and rules for governing resulting programs. The PEO/PM describes for the IRB the net-centric descriptions and requirements from the solution architecture with which the program is compliant. The IRB then assesses how this interpretation aligns with the guidelines established by the DoD IEA.

The IRB should conduct its assessments using criteria derived from the DoD IEA to determine the compliance of an investment or program with the Department's net-centric goals and objectives. The IRB can use applicable DoD IEA Priority Areas to determine the net-centric priorities the investment or program should be addressing and the associated net-centric requirements the investment or program should be following. The applicable Priority Area descriptions and those of associated net-centric capabilities from applicable capability and component architectures can provide the DoD CIO with a common context for understanding how the investment or program can be expected to operate in a net-centric DoD IE. This context can be used to develop measures for determining how well the investment or program is likely to perform in such an environment.

The IRB should extract certification criteria from the DoD IEA's Global Principles, as well as from Principles and Rules related to applicable Priority Areas. Applicable Rules, used in conjunction with associated Priority Area descriptions, extend net-centric capability descriptions to provide more detailed requirements for use in determining if capabilities to be

delivered by the investment or program will meet related net-centric goals, objectives, and needs.

Supplemental requirements and guidelines for use by the IRB in certification might also be gleaned from the net-centric concepts of technical federation, SOA, and technology innovation. These concepts contain best practices for enabling net-centric information sharing and should be applied in the context of the DoD IE. Criteria based on the elements of these concepts could be used to measure how well an investment can be expected to deliver the desired best practices. The context provided by these concepts could also be used to assist in selecting, refining, or extending the DoD IEA Principles and Rules to better assess net-centric capabilities to be delivered by the investment or program.

The IRB CONOPS says “the IRB Annual Review process is geared to highlighting issues related to delivery of capabilities as promised.” As with the investment certification process, capability and component architectures, aligned with the DoD IEA, provide standards for net-centric information sharing against which the DoD CIO should conduct the annual review. During the annual review, applicable DoD IEA Priority Areas, Principles, and Rules, coupled with descriptions of applicable net-centric capabilities, should be used to determine if programs are meeting net-centric requirements.

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

1. Introduction

Appendix E describes what compliance with the DoD Information Enterprise Architecture (IEA) means and ways to demonstrate and assess this compliance. As stated earlier, the DoD IEA provides a common foundation to support transformation of the DoD to net-centric operations. The common foundation is presented as a set of Principles and Rules that guide and constrain operations to facilitate a coherent movement towards net-centric operations. Appendix D, *Applying the DoD IEA*, addresses how to apply the DoD IEA. Appendix E describes the compliance areas and content that demonstrates compliance with the DoD IEA.

1.1 Application of DoD IEA Elements

Figure E-1, Application of the DoD IEA, illustrates how the primary elements of the DoD IEA (Priority Areas, Principles, Rules, Activities, Constraints, and Mechanisms) should be applied to a given architecture in the DoD Architecture Federation. The DoD IEA elements shown in the diagram as applicable to a specific architecture are considered the minimum necessary to describe interactions with the net-centric information environment at that level.

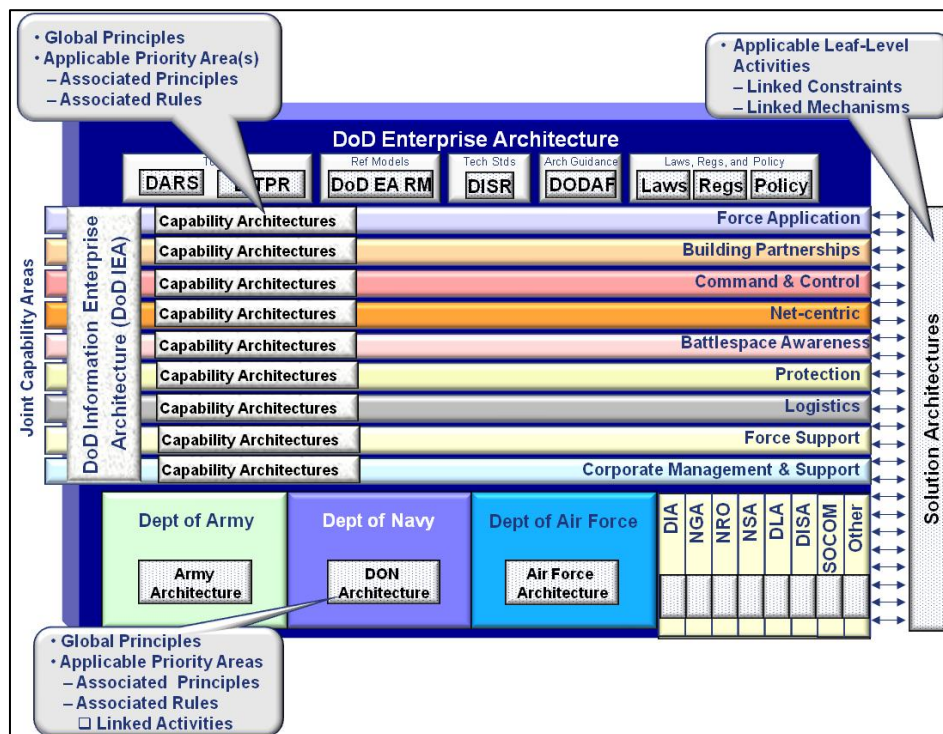


Figure E-8 - Application of the DoD IEA

This does not preclude use of additional DoD IEA elements to ensure a more complete, accurate, and/or detailed picture of the DoD IE to meet a given architecture's purpose, viewpoint, and scope. The DoD IEA elements discussed in this appendix apply to architectures as follows:

- Capability Architectures: Global Principles, applicable Priority Areas, associated Principles, and associated Rules
- Component Architectures: Global Principles, applicable Priority Areas, associated Principles, associated Rules, and linked Activities
- Solution Architectures: Applicable leaf-level Activities, linked Constraints, and linked Mechanisms

Appendix E is structured to align with Appendix D and the conceptual process provided for applying the DoD IEA. **Figure E-2**, Process for Applying DoD IEA to DoD Architectures, illustrates the conceptual process flow for applying the DoD IEA to the development, maintenance, and use of net-centric architectures.

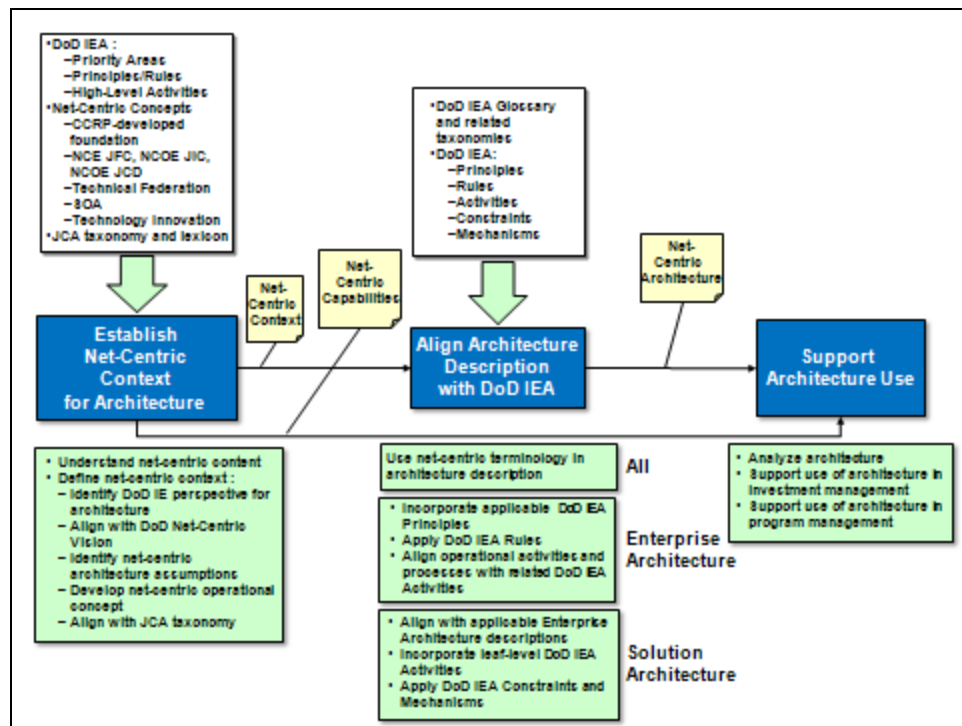


Figure E-9 - Process for Applying DoD IEA to DoD Architectures

Compliance areas described in this appendix align with appropriate sub-processes listed under the three main process steps in Figure E-2:

- **Establish Net-Centric Context for Architecture** - The architect identifies the portions of the Department's net-centric vision applicable to the architecture and applies the Net-Centric JCA and appropriate DoD IEA Priority Areas, Principles and Rules, and high level Activities to the development of a net-centric context for the architecture.
- **Align Architecture Description³¹ with the DoD IEA** - The architect develops an architecture description aligned with the DoD IEA. The architecture description uses net-centric terminology and applies appropriate DoD IEA Principles, Rules, and Activities.
- **Support Architecture Use** - The architect, in conjunction with program managers and decision-makers, analyzes governing architectures to develop a set of net-centric guidelines, based on DoD IEA Principles and Rules, to provide more detailed direction for program management and criteria for decision-making assessments. The architect then supports these stakeholders in using this net-centric guidance and information provided by the appropriate net-centric architecture descriptions in the development, acquisition, and deployment of required net-centric capabilities.

Table E-1, Appendix E Alignment with Appendix D, identifies the areas from Appendix D that will be discussed as Compliance Areas in Appendix E and the application paragraph they align with in Appendix D.

Table E-1 - Appendix E Alignment with Appendix D

Appendix D - Applying the DoD IEA		Appendix E -Compliance Areas
2.3.1 Establish Net-Centric Context for Architecture		
	2.3.1.1 Understand Net-Centric Concepts	
	2.3.1.2 Identify DoD IE Perspective of Architecture	* Identify DoD IE Perspective of Architecture
	2.3.1.3 Define Net-Centric Context	
	2.3.1.3.1 Align with DoD Net-Centric Vision	* Align with DoD Net-Centric Vision
	2.3.1.3.2 Identify Net-Centric Architecture Assumptions	* Identify Net-Centric Architecture Assumptions
	2.3.1.3.3 Develop a Net-Centric Operational Concept	* Develop a Net-Centric Operational Concept
	2.3.1.3.4 Align with JCA Taxonomy	* Align with JCA Taxonomy
2.3.2 Align Architecture Description with the DoD IEA		
	2.3.2.1 Alignment for All Architectures	* Alignment for All Architectures (Net-Centric Terminology)
	2.3.2.2 Alignment for Enterprise Architectures	
	2.3.2.2.1 Incorporate Applicable DoD IEA Principles	* Incorporate Applicable DoD IEA Principles
	2.3.2.2.2 Apply DoD IEA Rules	* Apply DoD IEA Rules
	2.3.2.2.3 Align Operations and Processes with Related DoD IEA Activities	* Align Operations and Processes with Related DoD IEA Activities
	2.3.2.3 Alignment for Solution Architectures	

³¹ DoDAF v1.5 (Volume I, p. 1-6) defines an architecture description as “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.”

	2.3.2.3.1 Align with Applicable Enterprise Architecture Descriptions	* Align with Applicable Enterprise Architecture Descriptions
	2.3.2.3.2 Incorporate Leaf-Level DoD IEA Activities	* Incorporate Leaf-Level DoD IEA Activities
	2.3.2.3.3 Apply DoD IEA Constraints and Mechanisms	* Apply DoD IEA Constraints and Mechanisms
	3. Application of DoD IEA in Program Management	* Program Compliance with the DoD IEA
	4. Application of DoD IEA in Decision-Making	* Evaluator and Decision-maker Perspective of Compliance with the DoD IEA

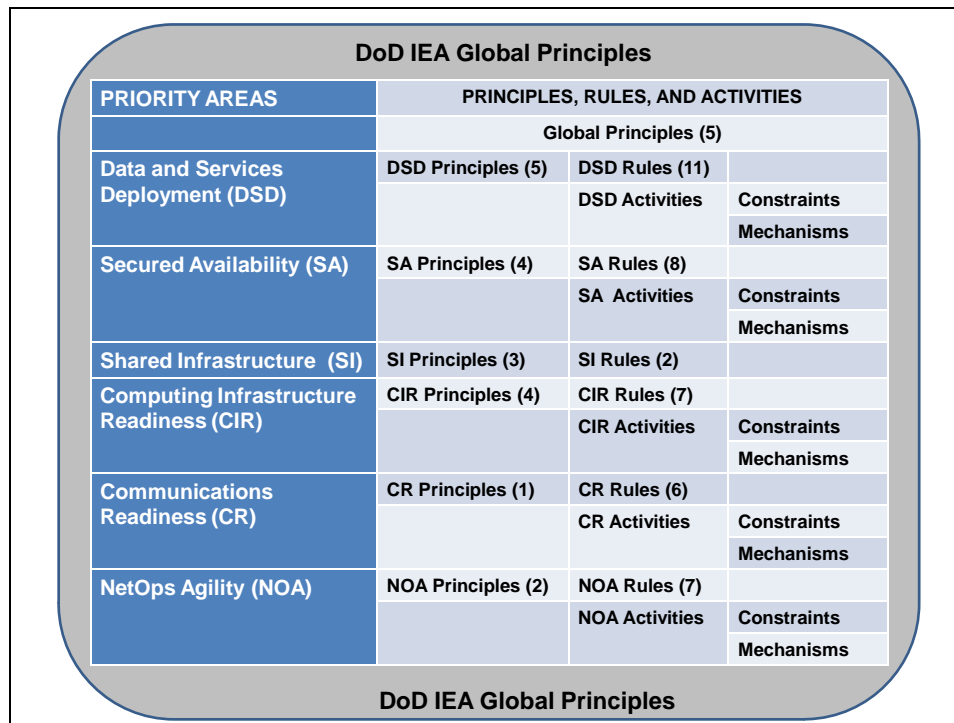
The Compliance Areas establish the scope and focus for complying with the DoD IEA and assessing Compliance.

1.2 The DoD IEA and the DoD Architecture Framework (DoDAF)

Adherence to the architecture descriptions of the DoDAF is essential for complying with the DoD IEA. The DoDAF describes the net-centric architecture constructs that are used to convey application of the DoD IEA Principles, Rules, Activities, Constraints, and Mechanisms. These net-centric architecture descriptions are necessary to demonstrate application of the DoD IEA and will be used to assess compliance with the DoD IEA. If DoDAF architecture descriptions are not available, compliance with the DoD IEA will be assessed using whatever descriptions are provided.

2. Compliance with the DoD IEA

Compliance with the DoD IEA has three perspectives. The first perspective, that of the IT architect, involves applying the DoD IEA and documenting its application in architecture descriptions. The second perspective, that of a Program and Portfolio Manager, involves describing how the Program or Portfolio complies with the DoD IEA. The third perspective, that of an Evaluator or Decision-maker, involves evaluating architecture, program, and portfolio compliance with the DoD IEA. Compliance means alignment with the DoD IEA Principles, Rules, and Activities. **Figure E-3** illustrates the general relationships among the DoD IEA Principles, Rules, and Activities. There are two types of Principles: Global Principles and Principles associated with the Priority Areas. The Rules are associated with the Priority Area Principles. The Activities are associated with the Priority Areas and the leaf-level Activities contain a set of associated Constraints and Mechanisms. Definitions for each element and the Activity decomposition can be found on the DoD IEA Website at <http://www.defenselink.mil/cio-nii/sites/diea/>.

Figure E-10 - DoD IEA Elements³²

A compliance template is used to organize descriptions of what Compliance with the DoD IEA entails. Familiarization with Appendix D, *Applying the DoD IEA*, will enhance the reader's understanding of the Compliance Template.

2.1 Compliance Template

The Compliance Template describes compliance from the perspective of an IT architect, Program and Portfolio Manager, and evaluator and decision maker. It provides compliance criteria, examples of demonstrating compliance, and guidance for evaluating compliance with the DoD IEA. 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 used. A Compliance Assessment Table containing key information from this Compliance Template and Appendix D is provided at Tab A³³. It can be used as a tool to monitor and track, or assess compliance with the DoD IEA.

³² The Shared Infrastructure (SI) Priority Area depicted in the diagram consists of relevant and applicable common infrastructure principles and business rules from the Computing Infrastructure Readiness (CIR), Communications Readiness (CR), and NetOps Agility (NOA) Priority Areas.

³³ TAB A at the end of Appendix E contains a compliance assessment table that contains key information for applying and complying with the DoD IEA. It also provides an area for architects or others to describe what DoD IEA content has been applied to and where it is located in the architecture.

2.1.1 Architecture Compliance with the DoD IEA

2.1.1.1 Establish Net-Centric Context for Architecture

Establishing a net-centric context for the architecture places the proper scope on the architecture to enable net-centric operations in support of interoperation across DoD.

2.1.1.1.1 Identify DoD IE Perspective of the Architecture

Identifying the DoD IE perspective of an architecture is part of the larger process for establishing a net-centric context. The importance of establishing a net-centric context for the architecture cannot be over emphasized. The net-centric context guides architecture development so the architecture properly presents net-centric characteristics appropriate to its purpose, viewpoint, and scope. Paragraph 2.3.1.2 of Appendix D, Applying the DoD IEA, contains descriptions for identifying the DoD IE perspective of an architecture.

There are three DoD IE perspectives: Producer/Provider, Manager, and Consumer of data and services. These perspectives determine the types of DoD IE interactions the architecture might describe. Most architecture will address a perspective as a Consumer of data and services given that most operations and activities use data and services during execution. Architectures may have more than one perspective. The perspectives of the architecture can be identified in the Architecture Viewpoint section of the AV-1 Overview and Summary Information product. As part of the architecture viewpoint, the AV-1 describes whether the architecture depicts a Data/Service Provider perspective, Data/Service Manager perspective, Data/Service Consumer perspective, or all.³⁴

2.1.1.1.2 Align with DoD Net-Centric Vision

Alignment with the DoD Net-Centric Vision is part of the larger process for establishing a net-centric context. The DoD IEA Priority Areas and associated Principles and Rules are applied to achieve the DoD Net-Centric Vision to function as one unified DoD enterprise 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.

Paragraph 2.3.1.3.1 of Appendix D, Applying the DoD IEA, contains descriptions for aligning with the DoD net-centric vision.

³⁴ DoD Architecture Framework (DoDAF) v1.5, Volume II, Product Descriptions, 23 April 2007, pg. 3-3. Paragraph 3.1.3 Net-Centric Guidance for AV-1 on page 3.2, describes the types of net-centric descriptions that can augment the AV-1 in a net-centric environment. The DoDAF focuses on provider and consumer perspectives. A manager perspective has been added to complete the picture.

Descriptions from the applicable Priority Areas and associated Principles and Rules may be used to express expected IE development, management, and use. These expectations can be expressed in the Context portion of the AV-1 to guide development of an architecture description.

These expectations may be expressed as early as possible in documents that define the IE enabling capabilities needed to support operational capabilities. IE capabilities, based on applicable DoD IEA Priority Areas, can be expressed in the Functional Area Analysis (FAA) as part of specifying conditions. These IE capabilities are then addressed in the Functional Needs Analysis (FNA) and Functional Solution Analysis (FSA). They can also be expressed in the operational concept of the Initial Capabilities Document (ICD) and the concept of operations summary of the Capability Development Document (CDD). The earlier these expectations are expressed in analyses and capabilities documents, the earlier the Net-Centric Vision is applied.

2.1.1.1.3 Identify Net-Centric Architecture Assumptions

Identifying net-centric architecture assumptions is part of the larger process for establishing a net-centric context. Net-centric assumptions for the architecture may be derived from the descriptions of the applicable DoD IEA Priority Areas and should encompass associated Principles and Rules. Paragraph 2.3.1.3.2 of Appendix D, Applying the DoD IEA, contains descriptions for identifying net-centric architecture assumptions.

Net-Centric architecture assumptions can be expressed in the AV-1. The assumptions may consider foundational policy, requirements associated with technical federation, SOA, and technology innovation. The assumptions should also take the perspectives of the architecture into account.

Assumptions supporting a consumer perspective are expressed differently than assumptions supporting a producer/provider perspective. Consider the Computing Infrastructure Readiness (CIR) Priority Area and associated Principles and Rules as an example. Potential assumptions supporting a consumer perspective are:

- Adequate processing and storage services are always available.
- User will have the ability to dynamically allocate computing resources in response to user needs.
- A secured and protected computing infrastructure.
- Computing infrastructure interfaces, provisioning, and allocation will be transparent to user.

Potential assumptions supporting producer/provider perspective are:

- All providers will comply with established interfaces and protocols
- Foundational infrastructure will be in place to support what is being provided
- Information Assurance (IA) requirements will be applied throughout development

A potential assumption that supports a manager perspective is that all infrastructure components will be developed to facilitate agile management.

2.1.1.1.4 Develop a Net-Centric Operational Concept

Developing a net-centric operational concept is part of the larger process for establishing a net-centric context. This is done by incorporating the net-centric vision of the DoD IEA into operational concepts. Paragraph 2.3.1.3.3 of Appendix D, Applying the DoD IEA, contains descriptions for developing a net-centric operational concept.

A net-centric operational concept can be expressed in architecture and related documents to scope and guide net-centric operations in the DoD IE. In an architecture, descriptions from applicable DoD IEA Priority Areas, Principles, Rules, and high-level Activities can be reflected graphically and textually in the High-Level Operational Concept (OV-1). These descriptions should be detailed enough to orient and focus net-centric concepts, capabilities, and interactions. A net-centric OV-1 depicts how the subject architecture uses an integrated, fully netted environment to execute the mission. The OV-1 is more than just a graphical depiction of the operational concept. It should include as much text description as necessary to clearly explain all aspects of the operational concept. The use of descriptive text, especially for a net-centric architecture, is needed to clearly describe the dynamic concepts associated with net-centric operations.

Descriptions from applicable DoD IEA Priority Areas, Principles, Rules, and high-level Activities can also be incorporated into the operational concept descriptions of a tailored Information Support Plan (ISP) as developed using the the Enhanced Information Support Plan (EISP) tool. As with the net-centric vision discussed earlier, the net-centric operational concept should be expressed as early as possible in FAAs, when appropriate. It can also be expressed in the operational concept of the Initial Capabilities Document (ICD) and the concept of operations summary of the Capability Development Document (CDD).

2.1.1.1.5 Align with Joint Capability Area (JCA) Taxonomy

Aligning with the Net-Centric JCA is a part of the larger process for establishing net-centric context. Alignment is accomplished by identifying capabilities from the Net-Centric JCA that are relevant to an architecture description. Paragraph 2.3.1.3.4 of Appendix D, Applying the DoD IEA, contains descriptions for aligning with the Net-Centric JCA.

Net-Centric JCA capabilities relevant to the architecture can be expressed in several ways. Descriptions of the relevant capabilities can be articulated in the Context portion of the AV-1

indicating whether the capability is provided or consumed. The capability descriptions can also be expressed in the OV-1 as part of the net-centric operational concept. If the architecture describes provisioning of a capability, the descriptions may be incorporated directly into the definition of the capability. If the capability is defined via activities, Net-Centric JCA descriptions may be seen in the OV-5 Operational Activity Model. If it describes consumption of a capability, the architecture may model the consumption or use of the capability. If this is the case, the descriptions may be provided in the OV-5 and the OV-6c Operational Event-Trace Description.

The Net-Centric JCA contains five tiers of capabilities with more tiers expected. It is important to incorporate capabilities at the appropriate tier depending upon the context of the architecture and the desired level of detail.

2.1.1.2 Align Architecture Description with the DoD IEA

2.1.1.2.1 Use Net-Centric Terminology

Using net-centric terminology in an architecture description is part of the larger process of aligning an architecture with the DoD IEA. The DoD IEA is one of many sources for net-centric terminology. The terminology exists in various approved vocabularies and taxonomies associated with COIs, Net-Centric Strategies, Capabilities, and other sources. Paragraph 2.3.2.1.1 of Appendix D, Applying the DoD IEA, contains descriptions for using net-centric terminology in an architecture description.

Net-centric terminology from the DoD IEA can be documented in the AV-2 Integrated Dictionary as well as developed taxonomies. It can also be expressed throughout the architecture in descriptions and definitions of net-centric capabilities and the DoD IE. The intent is not just to use net-centric terms, but to use them appropriately to articulate the application of the DoD IEA Principles, Rules, and Activities in describing the DoD IE in an architecture description. The ISP is a key document for expressing net-centric terminology in describing the DoD IE.

2.1.1.2.2 Incorporate Applicable DoD IEA Principles

Incorporating applicable DoD IEA Principles is part of the larger process for aligning architecture description with the DoD IEA. Incorporation of applicable Principles should focus on articulating an organization's intentions to provide a common basis for design and investment decisions. Paragraph 2.3.2.1.2 of Appendix D, Applying the DoD IEA, contains descriptions for incorporating applicable DoD IEA Principles in an architecture.

The perspective of the architecture plays a role in determining how Principles are expressed. A provider and manger perspective express the application of Principles to constrain and guide the development, delivery, and operation of DoD IE data and services. A consumer perspective expresses the application of Principles as guidelines for accessing and using data and services.

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.

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 exhibited 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 E-2** provides an example of this using an activity from the IA Integrated Architecture.

Table E-2 - 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. <i>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.</i>

In Table E-2, the activity and definition at the top of the table is an actual activity from the IA GIG Integrated Architecture.³⁵ 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 IDEF modeling notation, the application of a Principle can be expressed as a

³⁵ Information Assurance (IA) Component of the GIG Integrated Architecture, Increment 1, v1.1, 16 Nov 2006, pg. 3-25.

Control directly on the activity. **Figure E-4**, Expressing Principles as Controls on Activities, illustrates this method of expression.

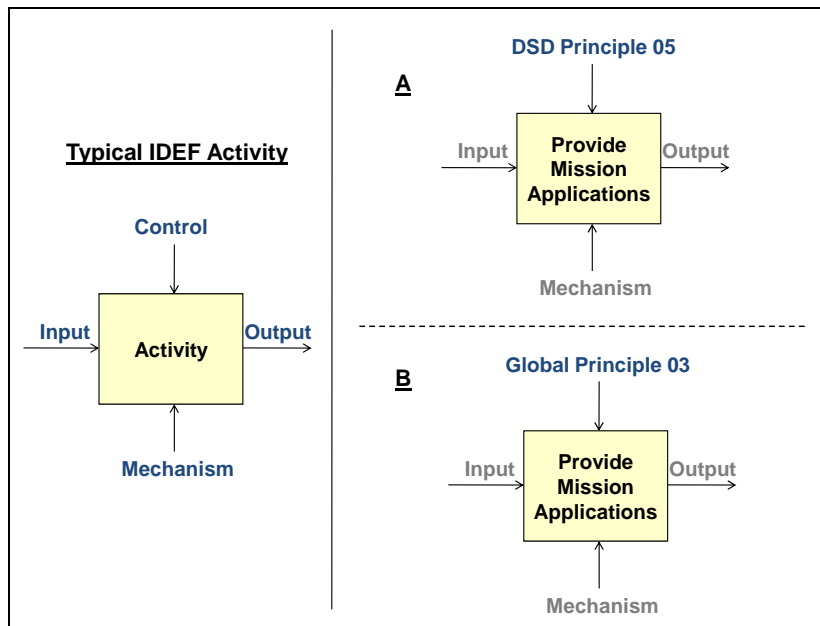


Figure E-11 - Expressing Principles as Controls on Activities

In Figure E-4, 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.*” 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.

2.1.1.2.3 Apply DoD IEA Rules

Applying DoD IEA Rules is part of the larger process for aligning architecture description with the DoD IEA. The DoD IEA Rules are definitive statements that define or constrain some aspect of the DoD IE. They are designed to drive common solutions and promote consistency across DoD programs, applications, and services. Paragraph 2.3.2.2.1 of Appendix D, Applying the DoD IEA, contains descriptions for applying DoD IEA Rules.

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:³⁶

- 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.”
- Action Assertion - “Establish a valid pedigree for data sources before declaring them as authoritative.”

³⁶ DoD Architecture Framework, v1.5, Volume II: Product Descriptions, 23 April 2007, pgs. 4-54 to 4-55.

- 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 and Services Rules Model. In contrast to the OV-6a, SV-10a focuses on constraints imposed by some aspect of operational performance requirements that translate into system performance requirements.³⁷ 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.”

2.1.1.2.4 Align Operational Activities and Processes with Related DoD IEA Activities

Aligning operational activities and processes with related DoD IEA activities is part of the larger process for aligning an architecture description with the DoD IEA. Applicable activities are identified based on the net-centric operational concept, applicable Priority Areas, and the architecture’s purpose regarding technical federation, SOA, and technology innovation. Paragraph 2.3.2.2.2 of Appendix D, Applying the DoD IEA, contains descriptions for aligning operational activities and processes with related DoD IEA activities.

The perspective(s) of the architecture is key in determining how alignment of operations and processes with related DoD IEA activities is expressed. To support a provider or manager perspective, operational activities and processes derived from applicable 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 E-5, 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 A15-Develop Design Patterns for Data and Services as the applicable Activity. It is defined as “This activity delivers data and services in a manner that is useful and meaningful to the end user.”

³⁷ DoD Architecture Framework, v1.5, Volume II: Product Descriptions, 23 April 2007, pg. 5-71.

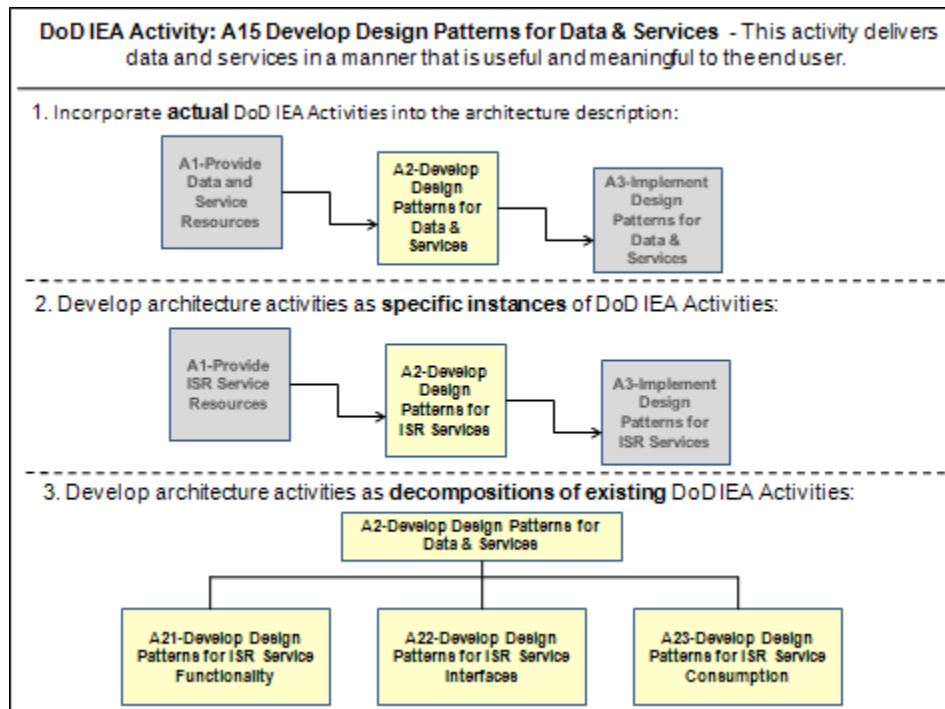


Figure E-12 - Examples for Expressing DoD IEA Activities in the OV-5

The first example in Figure 5 incorporates DoD IEA Activity A15 Develop Design Patterns for Data & Services as activity A2 of the architecture's OV-5. The second example expresses the DoD IEA Activity A15 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 A15 that fits the purpose of the architecture's OV-5.

A consumer perspective focuses on the Activities associated with the DSD Priority Area that describe how to use data and services in the DoD IE. Applicable Activities can be included in the descriptions of architecture activities in the OV-5, incorporating them as tasks performed to complete the activity. For process models, applicable Activities may be displayed in process flows, linked to process steps, or assembled into sub-processes as integral parts of the process.

2.1.1.2.5 Align with Applicable Enterprise Architecture Descriptions

Solution Architectures are typically associated with a specific Community of Interest (COI) based on the purpose and scope of the architecture. Solution architectures align with the DoD IEA first by aligning with the higher-level architectures governing and guiding their COI since these architectures have already aligned with the DoD IEA and provide the necessary community context. If Solution Architectures identify gaps that are not addressed by higher-level architectures associated with the COI, they should address the gaps by aligning directly with the DoD IEA. Paragraph 2.3.2.3.1 of Appendix D, Applying the DoD IEA, contains descriptions for aligning with higher-level architecture associated with the COI.

2.1.1.2.6 Incorporate Leaf-Level DoD IEA Activities

Leaf-level DoD IEA Activities may be incorporated into solution architectures given a need for additional detail. They may be used as the basis for decompositions providing more detailed activities or functions describing how the solution functions in the DoD IE. Paragraph 2.3.2.3.1 of Appendix D, Applying the DoD IEA, contains descriptions for incorporating leaf-level DoD IEA activities into architecture descriptions.

As a basis for more detailed decompositions, the leaf-level DoD IEA Activities may be expressed as activity or function decompositions in the OV-5 or SV-4b Services Functionality Description. In a net-centric architecture, the SV-4b is used to document service functionality that is exposed to the net-centric environment, their respective grouping into service families, and their service specifications. The SV-4b depicts how services are orchestrated together to deliver functionality associated with an operational need.³⁸

DoD IEA Activity A2851-Manage Subject Attribute Model Development is defined as “*This activity allows SA authorities to define a standard attribute model for DoD people, services, and property that supports attribute-based access control.*” This activity is about establishing a standard attribute model to support access control. **Figure E-6**, Incorporating Leaf-Level DoD IEA Activities into Architecture Descriptions, provides two examples of using activity A2851 as a basis for a more detailed activity decomposition and function decomposition.

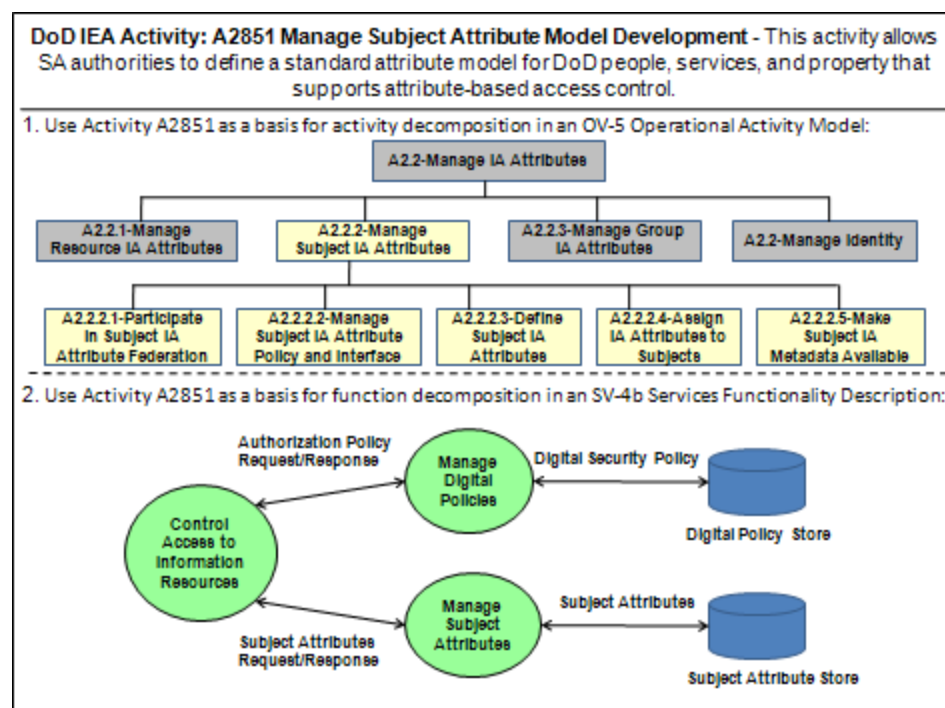


Figure E-13 - Incorporating Leaf-Level DoD IEA Activities into Architecture Descriptions

³⁸ DoD Architecture Framework, v1.5, Volume II: Product Descriptions, 23 April 2007, pg. 5-32. The SV-4b is the counterpart to the OV-5 as the SV-4a correlates to the SV-1 and SV-2.

The first example in Figure 6 is an actual activity decomposition from the Information Assurance (IA) GIG Integrated Architecture.³⁹ The IA activity A2.2.2-Manage Subject IA Attributes provides more detailed activity decomposition in an OV-5 that can be associated to the DoD IEA Activity A2851. The second example is a function decomposition from the same IA Architecture.⁴⁰ It provides a service functionality description for Access Control that includes the function of managing subject attributes, which is associated with the DoD IEA Activity A2851.

2.1.1.2.7 Apply DoD IEA Constraints and Mechanisms

Constraints and Mechanisms are linked to specific Activities in the DoD IEA Activity Decomposition. The Constraints are used to control the execution of the Activity and the Mechanisms are used as tools for accomplishing the Activity. Paragraph 2.3.2.3.2 of Appendix D, Applying the DoD IEA, contains descriptions for applying DoD IEA Constraints and Mechanisms to architecture descriptions.

There are two primary ways to express DoD IEA Constraints and Mechanisms in architecture descriptions:

- As controls and mechanisms on activities in the OV-5
- By complying with the Constraints and Mechanisms in other OV, SV, and TV architecture descriptions

Mechanism 74-DoD IT Standards Registry (DISR) and Constraint 24-DoD Directive 8320.02, Data Sharing in a Net-Centric Department of Defense are linked to several DoD IEA Activities. They can be expressed as controls and mechanisms for activities as illustrated in **Figure E-7**, Expressing DoD IEA Constraints and Mechanisms as Controls and Mechanisms for an Activity.

³⁹ Information Assurance (IA) Component of the GIG Integrated Architecture, Increment 1, v1.1, 16 Nov 2006, pg. 3-19.

⁴⁰ Information Assurance (IA) Component of the GIG Integrated Architecture, Increment 1, v1.1, 16 Nov 2006, Annex B: IA System Function Interdependencies in the Context of the IA Operational Capability Areas (OCAs), pg. B-4.

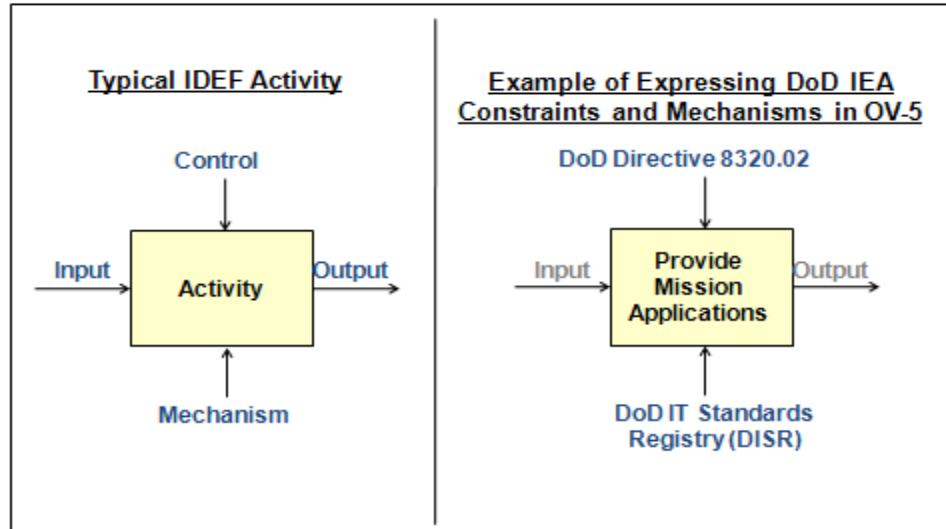


Figure E-14 - Expressing DoD IEA Constraints and Mechanisms as Controls and Mechanisms for an Activity

In this example, the activity Provide Mission Applications has the DoD Directive 8320.02 as a control and the DISR as a mechanism. Policy elements in the DoD Directive 8320.02 will control the execution of the activity Provide Mission Applications and content in the DISR (Standards, Technologies, etc) will be used to accomplish the activity.

Another way to express DoD IEA Constraints and Mechanisms in architecture descriptions is by complying with the content of the Constraint or Mechanism. One element of the DoD Directive 8320.02 states “Semantic and structural agreements for data sharing shall be promoted through communities (e.g., communities of interest (COIs)), consisting of data users (producers and consumers) and system developers, in accordance with reference (b).”⁴¹ Compliance with this element may be expressed in the SV-11 Physical Schema architecture description by defining the structure of the various kinds of system data that are utilized in the architecture description.

Compliance with the DISR may be expressed by describing appropriate standards and technologies from the DISR in the SV-9 Systems and Services Technology Forecast, TV-1 Technical Standards Profile, and TV-2 Technical Standards Forecast architecture descriptions.

2.1.2 Program Compliance with the DoD IEA

Section 3 of Appendix D, Applying the DoD IEA describes the application of the DoD IEA in Program Management. It describes how Program Executive Officers (PEO) and Program Managers (PM) can use solution architectures, properly aligned with the DoD IEA, in carrying out their responsibilities to accomplish objectives for program development, production, and sustainment.⁴² This section describes what compliance with the DoD IEA means to a PM.

⁴¹ DoD Directive 8320.02, December 2, 2004, Certified Current as of April 23, 2007, pg. 3.

⁴² The Defense Acquisition System, DoDD 5000.1, May 12, 2003.

The PM has overall responsibility for all aspects of a program from architecture development to system production, and the various program milestones and assessments that occur along the way. Program compliance with the DoD IEA begins with the development of an architecture to direct the program and application of the DoD IEA principles, rules and activities to this architecture, as discussed in Appendix D. Although architects develop such architectures, PMs are responsible for ensuring the architecture complies with the DoD IEA. An architecture that complies with the DoD IEA directly or indirectly via governing component architectures, provides system engineers necessary information and requirements to guide the design and development of a system that aligns with the DoD IEA principles and rules. The PM ensures the DoD IEA requirements described in the architecture are appropriately translated into concrete, physical system attributes and characteristics by the engineers. Program documents such as the Information Support Plan (ISP) and the Capability Development Document (CDD) are used to describe various aspects of the program. One aspect of the program the PM should document is the program's alignment with the DoD IEA. A PM should clearly describe the net-centric IE the program operates within by documenting the net-centric information attributes and characteristics of the program that result from aligning the program with the DoD IEA.

2.1.2.1 Information Support Plan

The Information Support Plan (ISP) documents interoperability, information, and supportability requirements and provides a means to assess the net-ready KPP (NR-KPP) for Joint Staff certification. Chapter 2 of the ISP provides an analysis of the sufficiency of IT support based on the operational and functional capabilities being supported.⁴³ The net-centric information attributes and characteristics of the program that are associated with the DoD IEA can be addressed in Chapter 2 of the ISP. Specifically, step ten of the thirteen step process for analysis requires the program to perform a net-centric assessment. Steps seven and eight are also relevant to addressing a program's net-centric information attributes.⁴⁴ The Enhanced ISP (EISP) tool, used to develop the ISP, provides questions that focus the analysis of IT support sufficiency; assists in articulating net-centric information attributes and characteristics; and assists in identifying potential issues.

The ISP provides a means for the PM to document the program's contribution to and interoperation in the DoD net-centric IE. If a program starts with a DoD IEA compliant architecture, and the architecture content is appropriately translated to physical system attributes, then the resulting system should properly contribute to and interoperate in the DoD net-centric IE. **Table E-3** shows a notional example of a DoD IEA rule as it transitions from architecture application to ISP documentation.

Table E-3 - DoD IEA Rule from Architecture to the ISP

1. DoD IEA Rule	DSD Rule 07: Services shall be advertised by registering with an
------------------------	--

⁴³ Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 30 June 2004, Pgs 79-80.

⁴⁴ Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 30 June 2004, Pgs 79-80.

	enterprise service registry.
2. Architecture Application	DSD Rule 07 is applied to architecture as an activity, “Register Services in Enterprise Service Registry” and as a process for registering services.
3. Translation to System Attribute	The activity and registration process in the architecture associated with DSD Rule 07 is translated to the following system attributes: - Interface with selected enterprise service registry - System functions to perform service registration process
4. ISP Documentation	The above system attributes are documented in Chapter 2 of the ISP. ISP documentation identifies enterprise service registry, interface with registry, and the system functions involved in the service registration process.

Rule 07 of the Data and Services Deployment (DSD) priority area is “Services shall be advertised by registering with an enterprise service registry.” In Table E-3, the architect applies DSD Rule 07 to architecture as an activity and a process model for registering [program] services in an enterprise service registry. System engineers translate the resulting architecture data to physical system attributes for design and development. The two system attributes identified are the interface to the enterprise service registry and the system functions used to execute the service registration process. The PM oversees the application of the DSD Rule 07 in the architecture; the translation of the architecture data to physical system attributes; and documents the system attributes and associated issues in the ISP.

2.1.2.2 Capability Documents

Capability documents can also be useful in describing net-centric aspects of a program. The Capability Development Document (CDD) provides the operational performance attributes, including KPPs, necessary to design a proposed system and guide the development and demonstration of the proposed increment.⁴⁵ While the ISP identifies a program’s net-centric information attributes and associated issues, the CDD defines authoritative, measurable, and testable capabilities needed by the warfighters to support system development and demonstration. The CDD establishes threshold and objective performance criteria for the NR-KPP which is mandatory for every program that exchanges information. Sections 3, 6, 8, and Appendix A of the CDD provide opportunities to address the net-centric information attributes of a program.⁴⁶

Section 3, Concept of Operations Summary, provides an opportunity to describe the enabling capabilities required to achieve the program’s desired operational outcomes. The net-centric information attributes of the program can be described as enabling capabilities.

⁴⁵ CJCSM 3170.01C, Operation of the Joint Capabilities Integration and Development System, 1 May 2007, Pg. F-2.

⁴⁶ CJCSM 3170.01C, Operation of the Joint Capabilities Integration and Development System, 1 May 2007.

Section 6, System Capabilities Required for the Increment, provides an opportunity to describe the net-centric information attributes as key system attributes (KSA) and NR-KPP. Descriptions of the KSA and NR-KPP include threshold and objective values.

Section 8, Information Technology and National Security Systems Supportability, provides an opportunity to identify the communities of interest (COI) the program is working with to make data visible, accessible, and understandable to other users on the GIG.

Appendix A, Net-Ready KPP Products, is a mandatory appendix that provides an opportunity to present architecture artifacts and statements regarding net-centric compliance (i.e., compliance with the DoD IEA) and the NR-KPP.

The PM has ample opportunities through the CDD, as well as the ISP, to document the net-centric information attributes of the program that result from applying the DoD IEA to architecture and appropriately translating architecture data to system attributes.

2.1.3 Evaluator and Decision-maker Perspective of Compliance with the DoD IEA

Evaluators and decision-makers have a perspective of compliance with the DoD IEA that differs from that of architects, engineers, and PMs. Architects, engineers, and PMs comply with the DoD IEA by applying the IT requirements (principles, rules and activities) to architecture and using it to guide system development. Evaluators assess or evaluate how well architectures and programs comply with DoD IEA IT requirements, and provide this compliance information to decision-makers. Decision-makers consider the DoD IEA compliance information, along with other information, in making investment and acquisition decisions.

Evaluators may examine architecture content, program documents (ISP and CDD), or both during the course of an assessment. Architects will apply the DoD IEA to architecture differently depending upon the purpose and scope of the architecture. When examining architecture content for evidence of compliance with the DoD IEA, the evaluator should look for content as described in Chapter 2.1.1.2 Align Architecture Description with the DoD IEA and the assessment table at TAB A of Appendix E. Ultimately, the evaluator wants to determine if the DoD IEA principles, rules and activities have been accounted for in the development of architecture. When examining program documents such as the ISP or CDD, evaluators should look for evidence of compliance with the DoD IEA as described in Chapter 2.1.2 Program Compliance with the DoD IEA.

Decision-makers will consider DoD IEA compliance information and reports provided by evaluators as one of the factors for investment and acquisition decision making.

Tab A to Appendix E: DoD IEA Compliance Assessment Table

Compliance Area	Appendix D Application Paragraph Reference	Appendix D Application of the DoD IEA	App E Compliance Paragraph Reference	Appendix E Compliance with the DoD IEA		Describe Content and Location of Demonstrated Compliance
				Compliance Description	DoDAF and Program Documents Examples	
A. Establish Net-Centric Context for Architecture						
A1. Identify DoD IE Perspective of the Architecture	2.3.1.2	Describe the DoD IE perspective as producer/provider, manager, consumer, or a combination of the three.	2.1.1.1.1	Describe the DoD IE perspective of the architecture.	Describe in the AV-1 Overview and Summary Information, Purpose and Viewpoint section.	
A2. Align with DoD Net-Centric Vision	2.3.1.3.1	- Identify applicable Priority Areas. - Determine how to address the Priority Areas to align with the DoD Net-centric vision. - Consider the perspective(s) of the architecture.	2.1.1.1.2	Describe the DoD IE of the architecture using DoD IEA Priority Area(s) descriptions.	Describe in the: - Functional Area Analysis (FAA) as part of specifying conditions. - Initial Capabilities Document (ICD) Operational Concept. - Capability Development Document (CDD) Concept	

Compliance Area	Appendix D Application Paragraph Reference	Appendix D Application of the DoD IEA	App E Compliance Paragraph Reference	Appendix E Compliance with the DoD IEA		Describe Content and Location of Demonstrated Compliance
				Compliance Description	DoDAF and Program Documents Examples	
					of Operations Summary.	
A3. Identify Net-Centric Architecture Assumptions	2.3.1.3.2	- Derive net-centric assumptions from the descriptions of applicable DoD IEA Priority Areas. - Consider foundational policy and applicable requirements associated with the technical federation, SOA, and technology innovation concepts.	2.1.1.1.3	Describe net-centric assumptions.	Describe in the AV-1 Overview and Summary Information, Architecture Project Identification.	
A4. Develop a Net-Centric Operational Concept	2.3.1.3.3	- Incorporate descriptions of appropriate DoD IEA Priority Areas, Principles, Rules, and high-level Activities into the operational concept.	2.1.1.1.4	Describe the DoD IE using applicable Priority Areas, Principles, Rules, and high-level Activities.	Describe in the: - OV-1 High-Level Operational Concept (Text and Graphics). - Information Support Plan (ISP)	

Compliance Area	Appendix D Application Paragraph Reference	Appendix D Application of the DoD IEA	App E Compliance Paragraph Reference	Appendix E Compliance with the DoD IEA		Describe Content and Location of Demonstrated Compliance
				Compliance Description	DoDAF and Program Documents Examples	
		- Describe how the DoD IE is used to enable net-centric operations in support of interoperation across DoD.			Operational Concept. - FAA as descriptions of IE capabilities. - ICD Operational Concept. - CDD Concept of Operations Summary.	
A5. Align with JCA Taxonomy	2.3.1.3.4	- Identify applicable Net-Centric JCA capabilities. - Incorporate descriptions of applicable Net-Centric JCA capabilities into the operational concept.	2.1.1.1.5	Describe applicable Net-Centric JCA capabilities.	Describe in the: - AV-1 Context. - OV-1 as part of a net-centric operational concept. - OV-5 Operational Activity Model. - OV-6c Operational Event Trace Description.	

B. Align Architecture Description with the DoD IEA						
B1. Use Net-Centric Terminology	2.3.2.1.1	Use key terms contained in the DoD IEA Glossary across architecture descriptions.	2.1.1.2.1	Describe applicable DoD IEA key terms.	Describe in the: - AV-2 Integrated Dictionary. - Related taxonomies. - ISP descriptions of the IE.	
B2. Incorporate Applicable DoD IEA Principles	2.3.2.2.1	<ul style="list-style-type: none"> - Identify applicable DoD IEA Principles and use in architecture descriptions to place restrictions or limitations on operations. - Use applicable Principles in operational concept descriptions. - Use applicable Principles as activities or in activity descriptions. - Use applicable Principles as controls on activity and process models. 	2.1.1.2.2	Describe DoD IEA Principles.	Describe in the: - OV-1 Operational Concept. - OV-5 Operational Activity Model. - Process Models	

B3. Apply DoD IEA Rules	2.3.2.2.2	<ul style="list-style-type: none"> - Identify applicable DoD IEA Rules and apply as constraints in architecture descriptions. - Incorporate DoD IEA Rules in activity, process, and service definitions. - Include Rules in architecture rules models. - Use Rules as a basis for more detailed technical rules. 	2.1.2.3	Describe applicable DoD IEA Rules.	Describe in the: <ul style="list-style-type: none"> - OV-5 activity definitions. - SV-1 service definitions. - Process model definitions. - OV-6a Operational Rules Model. - SV-10a Systems and Services Rules Model 	
B4. Align Operations and Processes with Related DoD IEA Activities	2.3.2.2.3	<ul style="list-style-type: none"> - Identify applicable DoD IEA Activities based on the net-centric operational concept, applicable Priority Areas, and the application of the technical federation, SOA, and technology innovation concepts. - Consider the 	2.1.2.4	Describe applicable DoD IEA Activities.	Describe in the: <ul style="list-style-type: none"> - OV-5 Operational Activity Model. - Process Model 	

DoD Information Enterprise Architecture 1.1

		<p>perspective(s) the architecture takes.</p> <ul style="list-style-type: none"> - Incorporate Activities directly in activity model. - Develop specific instances of applicable DoD IEA Activities. - Develop activity decompositions of DoD IEA Activities providing additional detail. 				
B5. Align with Applicable Enterprise Architecture Descriptions	2.3.2.3.1	<ul style="list-style-type: none"> - Incorporate relevant net-centric requirements from higher-level architecture descriptions. 	2.1.1.2.5	Solution architectures should align with the IE content from relevant higher-level architectures.	Use applicable architecture products to convey higher-level architecture alignment based on higher-level architecture content.	
B5. Incorporate Leaf-Level DoD IEA Activities	2.3.2.3.1	<ul style="list-style-type: none"> - Identify applicable DoD IEA leaf-level Activities. - Consider the architecture's purpose, viewpoint, scope, and perspective(s). 	2.1.1.2.6	Describe DoD IEA leaf-level Activities.	Describe in the: <ul style="list-style-type: none"> - OV-5 Operational Activity Model. - SV-4b Services Functionality Description. 	

DoD Information Enterprise Architecture 1.1

		<ul style="list-style-type: none"> - Use leaf-level Activities as a basis for more detailed activity and function decompositions describing how a solution operates in the DoD IE. 				
B6. Apply DoD IEA Constraints and Mechanisms	2.3.2.3.2	<ul style="list-style-type: none"> - Identify applicable DoD IEA Constraints and Mechanisms. - Apply Constraints to control activities and Mechanisms as tools to accomplish activities. - Comply with applicable Constraints using applicable Mechanisms to shape the solution description so it aligns with the DoD IEA. 	2.1.1.2.7	Describe DoD IEA Constraints and Mechanisms.	Describe in the: <ul style="list-style-type: none"> - OV-5 Operational Activity Model. - SV-9 Systems and Services Technology Forecast. - SV-11 Physical Schema. - TV-1 Technical Standards Profile. - TV-2 Technical Standards Forecast. 	

Appendix F: Mapping DoD IEA Activities to NCOW RM Activities

1. Introduction

Appendix F maps the DoD IEA activities to the NCOW RM activities providing a bridge to assist in transitioning from the NCOW RM to the DoD IEA. Prior to the DoD IEA, architectures and programs complied with the NCOW RM as directed by the CJCSI 6212.01D for the Net-Ready Key Performance Parameter (NR KPP).⁴⁷ Legacy architectures and programs incorporated activities from the NCOW RM to meet compliance criteria. Appendix F assists legacy architectures and programs comply with the DoD IEA by providing a mapping of previously used NCOW RM activities to the current DoD IEA activities. This appendix contains a table mapping the activities as well as a TAB for each of the three NCOW RM activity decompositions. **Table F-1** maps DoD IEA activities to NCOW RM activities. NCOW RM activities mapped to DoD IEA parent activities are potentially applicable to the associated DoD IEA child activities. NCOW RM parent activities that are mapped to the DoD IEA include their associated child activities as part of the mapping.

Table F-4 - DoD IEA Activities Mapped to NCOW RM Activities

DoD IEA LEVEL #	IEA ACTIVITY NAME	NCOW RM LEVEL #	RM ACTIVITY NAME
0	Defense Information Enterprise Architecture	E0	Evolve the Global Information Grid (GIG)
		CM0	Control and Manage the Global Information Grid (GIG)
		U0	Use the Global Information Grid (GIG)
1	Provide Data and Services Deployment	CM2.2.5	Manage Service Oriented Enterprise
		CM2.2.6	Manage Net-Centric Information Sharing
		E4.2	Provide Net-Centric Information Services
		E5.3.2	Institutionalize Enterprise Services
1.1	Provide Discovery Services	E3.3.3	Develop Information Capabilities
		E4.2.2	Provide Enterprise Services
1.1.1	Provide Data, Service and IT Resource Registration Services	CM2.2.6.3.1.2	Provide Enterprise Information Catalog
1.1.2	Provide Data, Service and IT Resource Search Services	CM2.2.6.3.1.4	Provide Search and Retrieval
1.2	Provide Core Enterprise	E3.3.1	Develop Enterprise Services

⁴⁷ CJCSI 6212.01D, Interoperability and Supportability of Information Technology and National Security Systems, 8 March 2006.

DoD Information Enterprise Architecture 1.1

DoD IEA LEVEL #	IEA ACTIVITY NAME	NCOW RM LEVEL #	RM ACTIVITY NAME
	Services		Capabilities
		E4.2.2	Provide Enterprise Services
		CM2.1.5	Administer Service Oriented Policy
1.2.1	Provide SOA Foundational Services		
1.2.2	Promote Data and Service Separation from Applications		
1.3	Provide Collaboration Services	E3.3.3	Develop Information Capabilities
		E4.2.2	Provide Enterprise Services
1.3.1	Provide Other Collaboration Services		
1.3.2	Provide Messaging Service		
1.3.3	Provide Awareness Services	CM2.2.6.3.1	Provide Information Awareness
1.4	Provide Common End User Interfaces	E3.2.3.1	Develop Semantic and Structural Information Agreements
		E4.2.1.1	Provide Service Interfaces
		E5.3.1.4	Respond to User Feedback
		U1	Interact Through Capability Interface
1.4.1	Provide Data In a Manner That Meets End User Needs	CM 2.2.6.3	Manage Information Dissemination and Content Staging
		U4.1	Associate Metadata to an Information Asset
		U4.2	Post Information Asset
1.4.2	Provide Flexible and Agile Services	E4.2.1	Provide Service
1.5	Develop Design Patterns for Data & Services	E5.3	Institutionalize Net-Centric Strategies
		CM2.1.3	Administer Sharing Policy
		U2	Access Services
		U4	Share Information
1.5.1	Ensure Services Follow Net-Centric Services Strategy	E2.2.2	Architect Enterprise Services Capabilities
		CM2.2.5	Manage Service Oriented Enterprise
1.5.2	Ensure Data Follows Net Centric Data Strategy	E2.2.1	Develop/Update Information Sharing Architectures
		CM2.2.6	Manage Net-Centric Information Sharing
1.5.3	Migrate Technologies to Standards	E3.1	Integrate Supporting Technologies
1.6	Foster Development for Standard Semantics	E3.2.3	Evolve Information Infrastructure
		CM2.2.6.2	Manage Net-Centric Information

DoD Information Enterprise Architecture 1.1

DoD IEA LEVEL #	IEA ACTIVITY NAME	NCOW RM LEVEL #	RM ACTIVITY NAME
			Sharing Resources
		CM2.1.3	Administer Sharing Policy
1.6.1	Coordinate Metadata for Data, Services and IT Resources	E3.2.3.1	Develop Semantic and Structural Information Agreements
		E4.2.1.3	Provide Service Metadata to GIG
		U4.1.1	Assign Metadata Values
1.6.2	Coordinate Communities Of Interest	CM2.2.6.1	Provide Communities of Interest
1.7	Enable Trust	E3.3.2	Develop Assurance Capabilities
		E4.1.3	Provide Assurance Infrastructure
		CM2.2.2	Manage Trust Relationship
		U3	Protect a Resource
1.7.1	Manage Integrity	U3.3	Provide Integrity
1.7.2	Manage Pedigree	E3.2.3.2.3	Define Authoritative Sources
		U3.5	Provide Non-repudiation
2	Provide Secured Availability	E1.1.3.2	Define IA Strategies, Policies, and Plans
		E2.1.3.2	Architect the IA Infrastructure
		E2.2.3	Architect Assurance Capabilities
		E3.2.4	Evolve Assurance Infrastructure
		E4.2.3	Provide Assurance Services
2.1	Provide Secure Transfer Services (CDS)	E5.3.1	Institutionalize Net-Centric Information Sharing Capabilities
		CM2.1.3.1	Administer Cross Domain Sharing Policy
		U4.3	Prepare Information for Sharing Across Security Domains
2.1.1	Issue and Administer Information Discovery Initiatives		
2.1.2	Issue and Administer Information Transfer Initiatives	E3.2.3.1.2	Define Interoperability Specifications
2.1.2.1	Oversee CDS Initiatives		
2.1.2.1.1	Manage Data Types Definitions		
2.1.2.1.2	Oversee E2E Solution Implementation		
2.1.2.2	Oversee DoD Migration from P2P to E2E Accreditation		

DoD Information Enterprise Architecture 1.1

DoD IEA LEVEL #	IEA ACTIVITY NAME	NCOW RM LEVEL #	RM ACTIVITY NAME
2.2	Provide Enclave, Network and Boundary Protection	E1.1.3	Develop Assurance Strategies, Policies and Plans
		E2.1.3	Architect the Assurance Infrastructure
		E2.2.3	Architect Assurance Capabilities
		E3.2.4.1.1.2	Engineer Network Protection Capabilities
		CM2.1.2	Administer Protection Policy
2.2.1	Provide Technical Protection Standards	E2.3	Architect Supporting Technologies
		E3.1	Integrate Supporting Technologies
		E3.2.2.1	Develop System Protection Capabilities
2.2.2	Provide Protection Architectures	E3.2.4.1.1.5	Define Network Demarcations, Authorities and Responsibilities
2.3	Provide Network Resource Management Mechanism Protection	E3.2.2.1	Develop System Protection Capabilities
		CM2.1.2	Administer Protection Policy
		CM2.1.4	Administer Network Management Policy
		CM2.2	Manage GIG Resources
2.4	Provide C&A Services	E1.1.3.2	Define IA Strategies, Policies and Plans
		E2.1.3.2	Architect the IA Infrastructure
		E2.2.3	Architect Assurance Capabilities
		E3.2.4.2	Evolve IA Infrastructure
		E3.2.4.1.2.5	Provide Certification and License Training Resources
		E4.2.3	Provide Assurance Services
2.4.1	Govern GIG-Wide C&A	E5.2	Control Capability Increment Integration
2.4.1.1	Manage/Provide Automated C&A Services		
2.4.2	Oversee Development of Unified C&A Standards and Processes		
2.4.2.1	Oversee Development of a DoD C&A Migration Strategy		
2.5	Provide IA Workforce	E3.4.1	Provide IA Training and Awareness
2.5.1	Oversee Identification of IA Positions		
2.5.2	Oversee Identification, Tracking, and Management of IA Personnel		

DoD Information Enterprise Architecture 1.1

DoD IEA LEVEL #	IEA ACTIVITY NAME	NCOW RM LEVEL #	RM ACTIVITY NAME
2.5.3	Oversee DoD IA Training and Education		
2.5.4	Promote GIG User Awareness		
2.5.5	Provide IA Tools and Services		
2.6	Provide IT Platform Protection		
2.6.1	Manage/Provide Integrated Assessment Process	E5.2.2	Certify Integrated Capability
		E5.2.3	Accredit Integrated Capability for Operation
2.6.2	Participate in Developing National E/P Acquisition Standards		
2.7	Provide Assured Control of the GIG	E1.1.3.1	Define NetOps Strategies, Policies, and Plans
		E1.1.3.2	Define IA Strategies, Policies, and Plans
		E.3.2.4.1.2.1	Develop Integrated NetOps Monitoring and Response Capabilities
		E4.1.3	Provide Assurance Infrastructure
		E4.2.3	Provide Assurance Services
		CM2.1.2.3	Administer CND Policy
		CM2.2.1	Manage IA Resources
		CM2.2.4	Manage Systems and Networks
2.7.1	Manage CND&IA Services	E3.2.4.1.2.2	Develop Integrated NetOps Management Capabilities
		E3.2.4.1.2.3	Define Status Reporting Requirements
		E3.2.4.1.2.4	Develop System and Network Logistics
2.7.2	Provide Configuration and Policy Based Management		
2.7.2.1	Manage Technology and Infrastructure		
2.7.2.2	Provide Policy Architecture		
2.7.2.3	Oversee Operational Management Process		
2.8	Provide Identity, Authentication, and Privilege Management	E3.2.4.2	Evolve IA Infrastructure
		E3.3.2	Develop Assurance Capabilities
		E4.1.3	Provide Assurance Infrastructure
		E4.2.3	Provide Assurance Services
		E5.3.3	Institutionalize Information Assurance
2.8.1	Develop Adaptive Access	CM2.1.1	Administer Access Control

DoD Information Enterprise Architecture 1.1

DoD IEA LEVEL #	IEA ACTIVITY NAME	NCOW RM LEVEL #	RM ACTIVITY NAME
	Framework		Policy
2.8.2	Manage IA&PM Policy Evolution	E1.1.3.2	Define IA Strategies, Policies and Plans
		CM2.1.1	Administer Access Control Policy
2.8.3	Oversee Identity Management Initiatives	E5.2	Control Capability Increment Integration
		CM2.1.1.2	Administer Identity Policy
2.8.3.1	Managing Identity Life Cycles		
2.8.3.2	Manage Credentialing Process	CM2.1.1.3	Administer Credential Policy
		CM2.2.1.2	Manage Credentials
2.8.4	Oversee Authentication Initiatives	E5.2	Control Capability Increment Integration
		CM2.1.1.5	Administer Authentication Policy
2.8.4.1	Manage Authentication Processes	E5.2.2	Certify Integrated Capability
		E5.2.3	Accredit Integrated Capability for Operation
2.8.5	Oversee Privilege Management Initiatives	CM2.1.1.1	Administer Attributes Policy
		CM2.1.1.4	Administer Authorization Policy
		CM2.2.1.1	Manage IA Attributes
2.8.5.1	Manage Subject Attribute Model Development		
2.8.5.1.1	Manage Privilege Life Cycle Development		
2.8.5.2	Manage Attribute Repository		
2.9	Provide EIMS	E4.2	Provide Net-Centric Information Services
		E4.2.3	Provide Assurance Services
2.9.1	Oversee IA Crypto Binding Tool Initiative		
2.9.2	Oversee IA Metadata Tag Initiative		
2.10	Provide Data-In-Transit & Data-At-Rest Protection	U3	Protect a Resource
2.10.1	Provide Data-At-Rest Protection	U3.1	Analyze and Confirm Protection Requirements
		U3.2	Provide Confidentiality
		U3.3	Provide Integrity
		U3.5	Provide Non-repudiation
2.10.2	Oversee Development of an Evolution Strategy	E1.1.3.2	Define IA Strategies, Policies, and Plans
		E3.2.4.2	Evolve IA Infrastructure
		CM2.2.4.2	Manage System and Network Performance
		CM2.2.4.3	Manage System and Network

DoD Information Enterprise Architecture 1.1

DoD IEA LEVEL #	IEA ACTIVITY NAME	NCOW RM LEVEL #	RM ACTIVITY NAME
			Configurations
2.10.2.1	Manage IPV6 Migration Strategy		
2.10.2.2	Manage NIPRNET/Internet Integration Initiatives		
2.10.2.3	Manage System High-System Integration Initiatives		
2.10.2.4	Manage Component Architecture Integration Initiatives		
2.10.2.5	Manage Coalition Sharing Initiatives	CM2.1.3.1	Administer Cross Domain Sharing Policy
		CM2.2.3.2	Manage Federation Information Exchange Requirements
2.11	Provide for Federation	CM2.1.1.4.1	Participate in Authorization Federation
		CM2.1.1.5.1	Participate in Authentication Federation
		CM2.1.3.2	Administer Federation Policy
		CM2.2.3	Manage Federations
		CM2.2.1.2.1	Participate in Credential Federation
		CM2.2.1.3.1	Participate in Key Management Federation
		CM2.2.5.1.1	Manage the Federation of GIG Services
2.11.1	Manage DoD's Participation in Federation		
2.11.1.1	Manage Federation Rules		
2.11.2	Synchronize and Deconflict DoD IA Attributes	CM2.2.1.1.1.1	Participate in Resource Attribute Federation
		CM2.2.1.1.2.1	Participate in Subject Attribute Federation
		CM2.2.1.1.3.1	Participate in Group Attribute Federation
		CM2.2.1.1.4.1	Participate in Identity Federation
2.12	Manage Mission Assurance Processes	E3.3.2	Develop Assurance Capabilities
		E4.2.3	Provide Assurance Services
		E5.2	Control Capability Increment Integration
		E3.2.4.1.1.2	Engineer Network Protection Capabilities
		CM1.1	Maintain GIG Situational Awareness
		CM1.2.2	Assess Vulnerabilities of the GIG

DoD Information Enterprise Architecture 1.1

DoD IEA LEVEL #	IEA ACTIVITY NAME	NCOW RM LEVEL #	RM ACTIVITY NAME
		CM1.3	Plan Response to Situation
		CM1.4	Respond to Situation
		CM2.2.4	Manage Systems and Networks
2.12.1	Provide Software Assurance Process		
2.12.2	Provide Hardware Assurance Process		
2.12.3	Provide System Assurance Process		
2.12.4	Provide Supplier Assurance Process		
2.13	Provide for Globalization	E1	Guide and Direct Global Information Grid (GIG) Evolution
3	Provide Computing Infrastructure Readiness	E1.1.5	Develop Computing Strategies, Policies and Plans
		E2.1.2	Architect the Computing Infrastructure
3.1	Develop and Implement Computing Infrastructure	E3.2.2	Evolve Computing Infrastructure
		E2.1.2	Architect the Computing Infrastructure
3.1.1	Develop / Enforce Computing Standards	E2.3	Architect Supporting Technologies
		E3.1	Integrate Supporting Technologies
3.1.2	Acquire Computing Infrastructure Solution(s)	E5.2	Control Capability Increment Integration
3.1.3	Install Computing Infrastructure Solution(s)	E3.2.2.2	Develop Computer Hardware and Software Installation
3.1.4	Integrate Computing Infrastructure Solution(s)	E3.2.2.4	Define Administrative Domains, Authorities, and Responsibilities
3.1.5	Deploy Computing Infrastructure Solution(s)		
3.1.6	Test and Accredit Computing Infrastructure Solution(s)	E3.2.2.8	Test Computing Infrastructure
		E5.2.3	Accredit Integrated Capability for Operation
3.2	Provide Computing Infrastructure Net-Centric Environments	E4.1	Provide Net-Centric Infrastructure
		E4.2	Provide Net-Centric Information Services
		E4.3	Implement Net-Centric Processes
		E3.2.2	Evolve Computing Infrastructure
3.2.1	Provide Self Managing CI Operations	CM2.2.4	Manage Systems and Networks
3.2.1.1	Automate Computing Infrastructure Operations		

DoD Information Enterprise Architecture 1.1

DoD IEA LEVEL #	IEA ACTIVITY NAME	NCOW RM LEVEL #	RM ACTIVITY NAME
3.2.1.2	Support Data Fusion	CM1.1	Maintain GIG Situational Awareness
		CM2.2.4.6	Manage GIG Sensor Grid
3.2.1.3	Enable Dynamic GIG Processing Utilization		
3.2.2	Provide Hardware Environment	E3.2.2.2	Develop Computer Hardware and Software Installation
3.2.3	Provide Storage Environment	E3.2.2.6	Coordinate Establishing Content and Content Mapping
3.2.4	Provide Software Environment	E3.2.2.2	Develop Computer Hardware and Software Installation
		E3.2.2.5	Engineer System Software
3.2.5	Provide High Productivity Computing Infrastructure Environment		
3.2.6	Provide Autonomous Environment		
3.2.7	Provide Grid Computing Infrastructure Environment		
3.2.8	Provide Computing Infrastructure Services	E4.1.2	Provide Computing Infrastructure
		E4.2.2	Provide Enterprise Services
3.2.8.1	Provide Shared Computing		
3.2.8.2	Provide Computing Infrastructure Storage Services		
3.2.8.3	Provide Operating System (OS) Services		
3.2.8.3.1	Provide Runtime Services		
3.2.8.4	Provide Operation Oversight Services	E3.2.2.7	Develop Systems Management and Reporting Systems
3.2.8.5	Assess Computing Infrastructure Related User Needs		
3.2.9	Provide Application Migration Support		
3.2.10	Perform Computing Infrastructure Information Assurance (IA) Support	E3.2.2.1	Develop System Protection Capabilities
		E4.2.3	Provide Assurance Services
3.2.10.1	Perform CI IA Encryptions for Shared Storage and Media Functions		
3.2.10.2	Ensure Secure Interoperability	E3.2.3.1.2	Define Interoperability Specifications
		E3.2.2.6	Coordinate Establishing Content and Content Mapping

DoD Information Enterprise Architecture 1.1

DoD IEA LEVEL #	IEA ACTIVITY NAME	NCOW RM LEVEL #	RM ACTIVITY NAME
3.2.10.3	Provide Trusted Computing		
3.3	Provide Computing Infrastructure Controls		
3.3.1	Provide Security Control Mechanisms		
3.3.1.1	Provide Access Controls	CM2.1.1	Administer Access Control Policy
3.3.1.2	Provide Privilege Controls	CM2.1.1	Administer Access Control Policy
		CM2.2.4.3	Manage System and Network Configurations
3.3.1.3	Provide Hardware and OS Security Configuration Controls	CM1.2.2	Assess Vulnerabilities of the GIG
3.3.2	Perform Computing Infrastructure Configuration Management	CM2.2.4.3	Manage System & Network Configurations
3.3.3	Performance Management	CM2.2.4.2	Manage System and Network Performance
3.3.3.1	Develop and Apply CI Metrics for Testing and Development	E3.2.2.7	Develop Systems Management and Reporting Systems
		E3.2.2.8	Test Computing Infrastructure
3.3.3.2	Conduct Computing Infrastructure Performance Assessment	CM1.2.2	Assess Vulnerabilities of the GIG
3.3.3.3	Provide Optimization / Performance Controls	CM2.2.4.3	Manage System & Network Configurations
3.3.3.4	Parameterize GIG Resources		
3.3.4	Maintain Computing Infrastructure	CM2.2.4.1	Manage System and Network Faults
3.4	Allocate Computing Infrastructure Resources	CM1.4.3	Maintain Optimal GIG Performance
		CM2.2.4.2	Manage System and Network Performance
3.4.1	Allocate Computing Resources		
3.4.1.1	Allocate Shared Computing Resources		
3.4.1.2	Allocate Processing		
3.4.1.3	Allocate Operations Across Hardware Resources		
3.4.2	Allocate Storage Resources		
3.4.3	Allocate Network Interfaces		
3.4.4	Allocate Physical Facilities		
3.5	Facilitate Computing		

DoD Information Enterprise Architecture 1.1

DoD IEA LEVEL #	IEA ACTIVITY NAME	NCOW RM LEVEL #	RM ACTIVITY NAME
	Infrastructure Knowledge Management		
3.5.1	Provide Computing Infrastructure Metadata	CM2.2.6.2.4	Manage Discovery Metadata
		U4.2	Post Information Asset
3.5.1.1	Develop Computing Infrastructure Ontology	E3.2.3.1	Develop Semantic and Structural Information Agreements
		CM2.2.6.2.2	Manage Ontologies
3.5.1.2	Ensure Computing Infrastructure Metadata is Discoverable	U4.1.1.1	Assign Discovery Metadata Values
3.5.1.3	Provide Computing Infrastructure Functionality Information	E4.2.1.4	Provide Service Performance, Operational State and Availability to GIG
3.5.1.4	Provide Computing Infrastructure Capacity Information	E4.2.1.4	Provide Service Performance, Operational State and Availability to GIG
3.5.1.5	Provide Computing Infrastructure Asset Location Information	E4.2.1.2	Provide Service to GIG
		E4.2.1.3	Provide Service Metadata to GIG
		U4.1.1.3	Assign COI-Specific Metadata Values
3.5.2	Provide Computing Infrastructure Support to NetOps	E3.2.4.1.2	Develop NetOps Support Capabilities
3.5.2.1	Provide Computing Infrastructure Availability Information	E3.2.2.7	Develop Systems Management and Reporting Systems
		E4.2.1.4	Provide Service Performance, Operational State and Availability to GIG
3.5.2.2	Provide Computing Infrastructure Access Information	U4.5.3	Acquire an Information Access Methodology
3.6	Evolve Computing Infrastructure	E3.2.2	Evolve Computing Infrastructure
3.6.1	Advance Computing Infrastructure Technology	E4.1.2	Provide Computing Infrastructure
3.6.1.1	Perform Technology Forecast	E2.1.2	Architect the Computing Infrastructure
3.6.1.2	Conduct Research and Development Efforts	E3.1.1	Develop Technologies
3.6.1.3	Determine Implication of Technology Development for DoD Mission	E3.1.2	Evaluate Technologies
3.6.2	Accomplish Computing Infrastructure Transition	E2.1.2	Architect the Computing Infrastructure

DoD Information Enterprise Architecture 1.1

DoD IEA LEVEL #	IEA ACTIVITY NAME	NCOW RM LEVEL #	RM ACTIVITY NAME
	Planning		
4	Provide Communications Readiness		
4.1	Support Interoperability of All GIG Components	CM2.2.6.2.3	Manage Interoperability Components
4.1.1	Support Interoperability Standards	E2.1.1	Architect the Transport Infrastructure
4.1.2	Support Technology Insertion, Reuse and Retirement	E3.2.1.1	Develop and Test NCOE
		E3.2.1.2	Develop and Test Tactical Reach-back
4.1.3	Allocate Electromagnetic Spectrum	E3.2.4.1.1.6	Develop Electromagnetic Frequency Assignments
		CM2.2.4.5	Manage Frequencies
4.1.3.1	Optimize Spectrum Use		
4.1.3.2	Support Compatibility with other Systems (e.g. Non GIG Systems)		
4.2	Provide Physical Connectivity	E3.2.1	Evolve Transport Infrastructure
		E4.1.1	Provide Transport Infrastructure
		CM2.2.4	Manage Systems and Networks
		U1	Interact Through Capability Interface
4.2.1	Support Enterprise Users		
4.2.2	Support Regional Users		
4.2.3	Support Deployed Users		
4.3	Support QoS Standards	E3.2.1	Evolve Transport Infrastructure
		E4.1.1	Provide Transport Infrastructure
		CM2.2.4	Manage Systems and Networks
4.3.1	Support Service Level Agreements (SLA)	E3.3.3.1	Define Service Levels
		CM2.2.4.2	Manage System and Network Performance
		CM2.2.4.3	Manage System and Network Configurations
4.3.2	Facilitate Continuity of Service	E3.2.4.1.1.8	Develop Continuity of Operations Planning
4.3.2.1	Support Reliability/Maintainability/Availability Standards		
4.3.2.2	Support System Redundancy		
4.3.3	Support Precedence Policies		
4.4	Plan Resource Allocation	E1.1.4	Develop Communications Strategies, Policies, and Plans
		E2.1.1	Architect the Transport Infrastructure
		CM2.2.4.4	Manage Satellite

DoD Information Enterprise Architecture 1.1

DoD IEA LEVEL #	IEA ACTIVITY NAME	NCOW RM LEVEL #	RM ACTIVITY NAME
			Communications Subsystems
		CM2.2.4.5	Manage Frequencies
4.4.1	Support Surge Loading		
4.4.2	Support Multiple Military Operations		
4.4.3	Support Day-to-Day Operations	CM1.4.3	Maintain Optimal GIG Performance
5	Provide NetOps Agility		
5.1	Expose GIG Situational Awareness Information	CM1.1.3	Provide Situational Awareness Data
		CM2.2.6.3.1	Provide Information Awareness
5.1.1	Publish GIG Situational Awareness Info	CM2.2.6.3.1.1	Provide Smart Push and Pull Capability
		CM2.2.6.3.1.2	Provide Enterprise Information Catalog
5.1.2	Subscribe GIG Situational Awareness Info		
5.1.3	Advertise GIG Situational Awareness Info	CM2.2.6.3.1.3	Advertise Catalog
5.2	Facilitate Assured Access to GIG Situational Awareness Information	CM2.1.1	Administer Access Control Policy
		CM2.2.6.3.2	Manage Information Access
		U2.6	Acquire Access Authorization to the Service
		U4.5.4	Acquire an Information Access Authorization
5.2.1	Manage Access Control	CM2.2.6.3.2.2	Manage Subscriber IDM Profile
		CM2.2.6.3.2.3	Manage IDM Access Controls
5.2.2	Create/Maintain Shared Space	CM2.1.3	Administer Sharing Policy
		CM2.2.6.3.3	Manage Information Delivery
5.3	Manage Information Exchange Resources	CM1.4.3	Maintain Optimal GIG Performance
		CM2.2.6.2	Manage Net-Centric Information Sharing Resources
5.3.1	Prioritize Information Infrastructure Demands	CM 2.2.6.2.1	Manage Information Sharing Infrastructure
		CM2.2.6.3.3.2	Prioritize Information Delivery
5.3.2	Optimize Information Infrastructure Use	CM2.2.6.3.3.3	Optimize Resource Use
		CM2.2.4.2	Manage System and Network Performance
		CM2.2.4.3	Manage System and Network Configurations
5.4	Produce Relevant GIG Situational Awareness	CM1.1	Maintain GIG Situational Awareness
5.4.1	Process GIG Situation Awareness Information	CM1.1.1	Acquire Situational Awareness Data

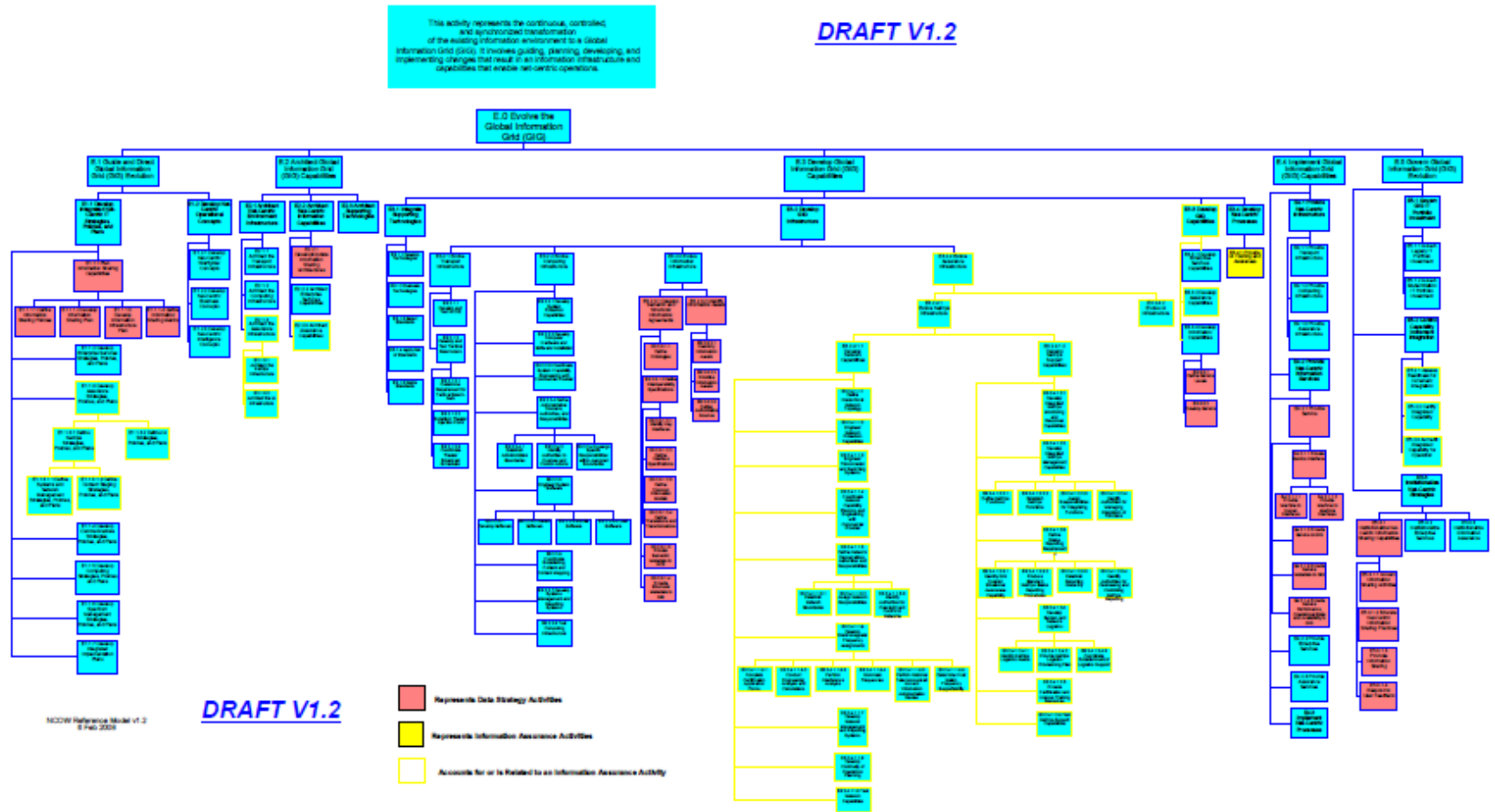
DoD Information Enterprise Architecture 1.1

DoD IEA LEVEL #	IEA ACTIVITY NAME	NCOW RM LEVEL #	RM ACTIVITY NAME
		CM1.1.2	Process Situational Awareness Data
5.4.2	Generate GIG Situational Awareness Info	CM1.1.3	Provide Situational Awareness Data
5.4.3	Create Tailorable Visualizations	CM1.1.3	Provide Situational Awareness Data
5.5	Perform Operational Control	CM1	Control the Global Information Grid (GIG)
5.5.1	Perform GIG Enterprise Management	CM2.2	Manage GIG Resources
5.5.2	Perform GIG Network Defense	CM1	Control the Global Information Grid (GIG)
5.5.3	Perform GIG Content Management	CM1.1	Maintain GIG Situational Awareness
		CM1.2	Assess GIG Situation
		CM2.2.6.3	Manage Information Dissemination and Content Staging
5.5.4	Develop Response to the GIG Situation	CM1.3.1	Identify Response Options
		CM1.3.2	Analyze Response Options
5.5.5	Select Response to the GIG Situation	CM1.3.3	Select Response
5.5.6	Coordinate Response to the GIG Situation	CM1.3.4	Coordinate Selected Response
5.5.7	Execute Response to the GIG Situation	CM1.4.1	Direct Response
		CM1.4.2	Execute Directed Response
5.6	Measure Effectiveness of the GIG	CM1.1.1	Acquire Situational Awareness Data
		CM1.2	Assess GIG Situation
5.6.1	Measure Operational GIG Effectiveness		
5.6.2	Measure Strategic GIG Effectiveness		
5.7	Manage Operational Policy	CM2.1	Administer GIG Policy
5.7.1	Administer NetOps Policies	CM2.1.2.3	Administer CND Policy
		CM2.1.4	Administer Network Management Policy
5.7.2	Monitor NetOps Policies	CM1.1	Maintain GIG Situational Awareness
		CM2.2.4	Manage Systems and Networks
5.7.3	Enforce NetOps Policies	CM1	Control the Global Information Grid (GIG)
		CM2.2.4	Manage Systems and Networks
5.8	Establish Commander's NetOps Intent		
5.8.1	Develop Commander's Intent		

DoD IEA LEVEL #	IEA ACTIVITY NAME	NCOW RM LEVEL #	RM ACTIVITY NAME
	for GIG NetOps		
5.8.2	Promulgate Commander's Intent for GIG NetOps		
5.8.3	Monitor Commander's Intent for GIG NetOps		
5.9	Plan GIG NetOps	E1.1.3.1	Define NetOps Strategies, Policies, and Plans
		CM1	Control the Global Information Grid (GIG)
5.9.1	Determine Requirements		
5.9.2	Develop Plans		
5.9.3	Coordinate Plans		
5.9.4	Implement NetOps Plans		
5.10	Evolve NetOps Capabilities	E3.2.4.1	Evolve NetOps Infrastructure
		E3.3.2	Develop Assurance Capabilities

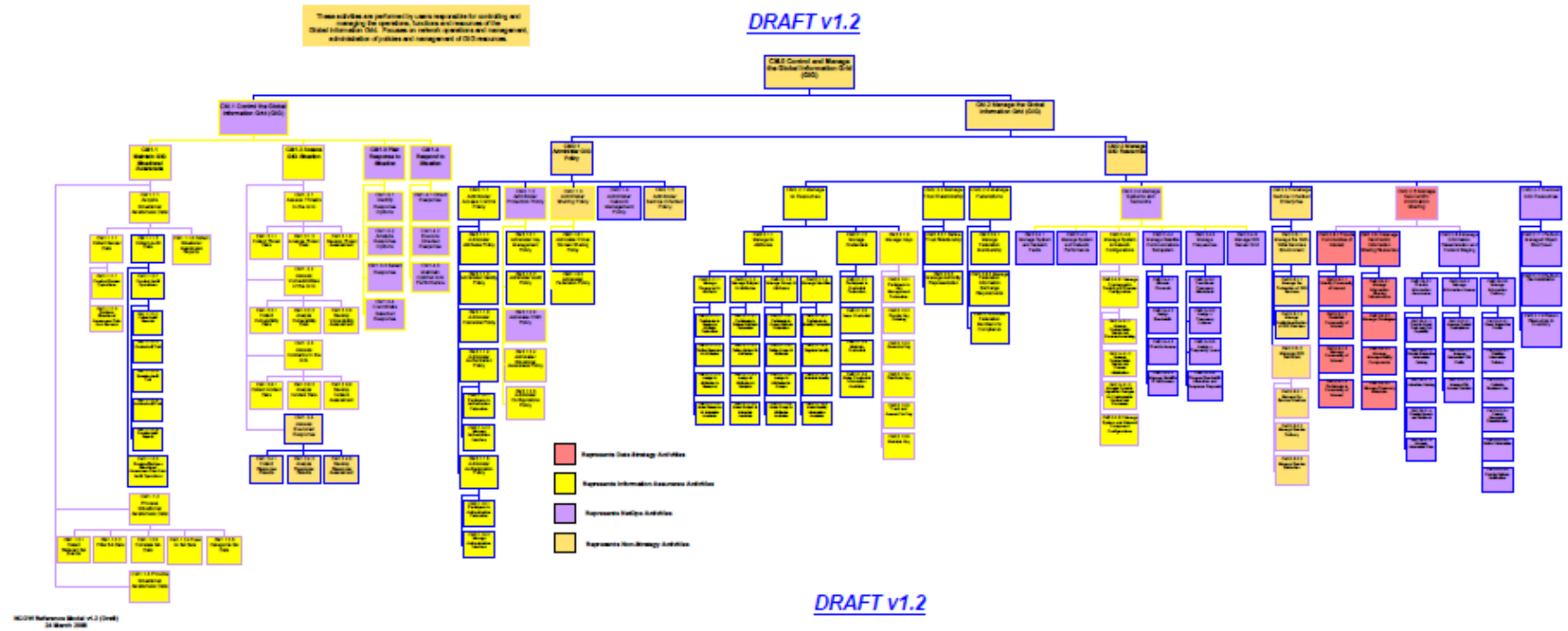
Tab A to Appendix F: NCOW RM Activity Decomposition - Evolve the GIG

18

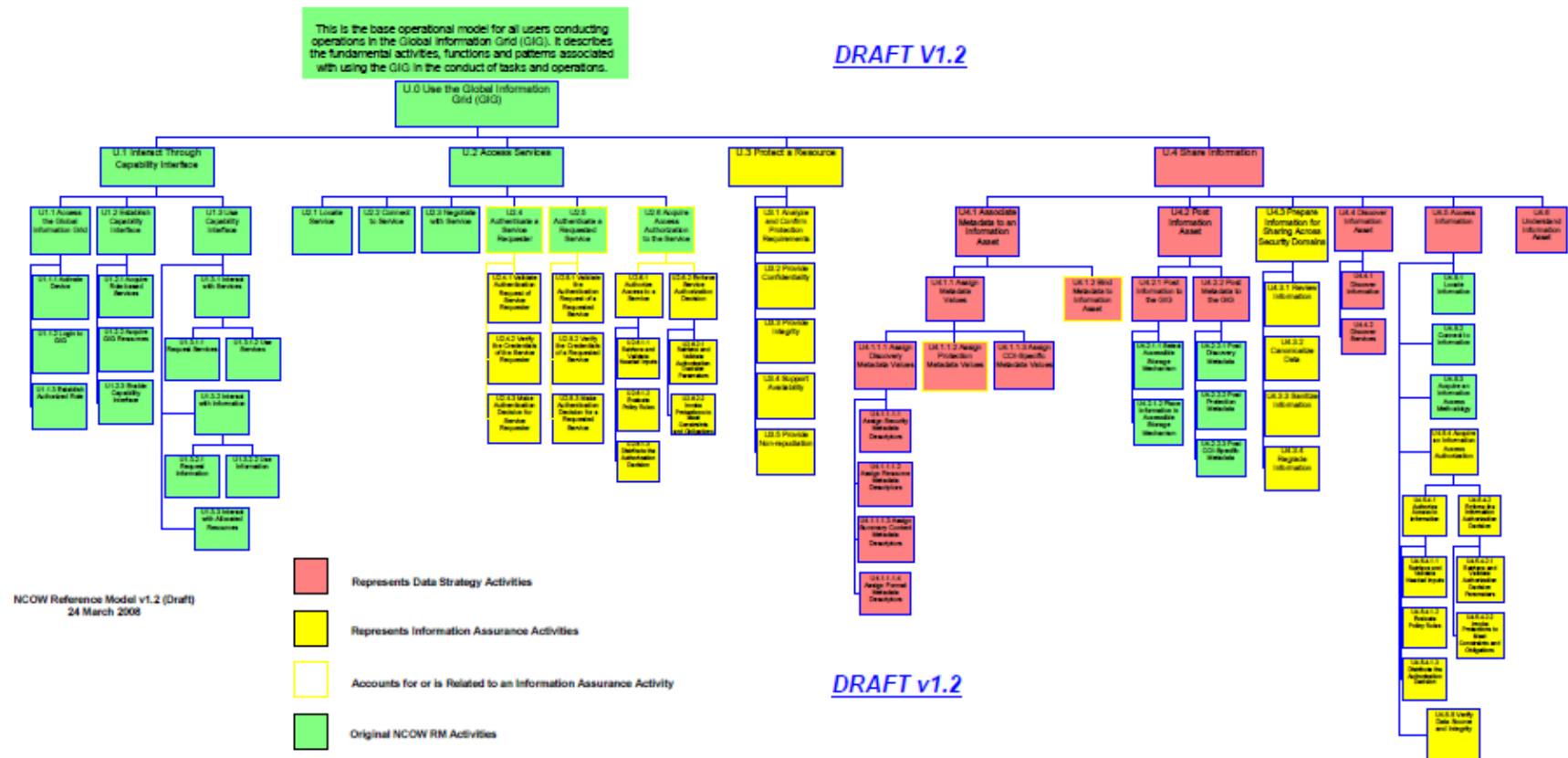


19
20
21

Tab A to Appendix F: NCOW RM Activity Decomposition - Evolve the GIG



Tab A to Appendix F: NCOW RM Activity Decomposition - Evolve the GIG



Appendix G: 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 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.

C4ISR Cooperative Research Project (CCRP): An organization within the Office of the Assistant Secretary of Defense (NII) that focuses on (1) improving both the state of the art and the state of the practice of command and control and (2) enhancing DoD's understanding of the national security implications of the Information Age. The CCRP pursues a broad program of research and analysis in command and control (C2) theory, doctrine, applications, systems, the implications of emerging technology, and C2 experimentation; develops new concepts for C2 in joint, combined, and coalition operations in the context of both traditional and non-traditional missions; and supports professional military education in the areas of C2, Information Superiority, network-centric operations, and related technologies.

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.

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. A DoD Information Enterprise Architecture priority.

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. A DoD Information Enterprise Architecture priority.

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: That 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).

A DoD Information Enterprise Architecture priority.

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 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 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.

Elements of DoD IEA: Priority Areas, Principles, Rules, Activities, Constraints, and Mechanisms.

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 Management: The functional capabilities and operational processes necessary to monitor, manage, and control the availability, allocation, and performance within and across the GIG. 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.

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, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

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

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 and facilities (DOTMLPF) and policy 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 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.

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. A DoD Information Enterprise Architecture priority.

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).

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. 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 (SOA): 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.

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

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, nonintelligence, raw, and processed) are advertised or “made visible” by providing metadata, which describes the asset.