

**Department of Defense
Defense Information Enterprise Architecture
Version 1.0**



April 11, 2008

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

(This page intentionally left blank)

EXECUTIVE SUMMARY

The Defense Information Enterprise Architecture (DIEA) 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 Defense Information Enterprise comprises the information, information resources, assets, and processes required to achieve an information advantage and share information across the Department and with mission partners. DIEA describes the integrated Defense Information Enterprise and the rules for the information assets and resources that enable it.

DIEA 1.0 unifies the concepts embedded in the Department's net-centric strategies into a common vision, providing relevance and context to existing policy. DIEA 1.0 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 DIEA 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 DIEA 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)

DIEA 1.0 enables DoD decision-makers to have informed discussions on key issues driving evolution of DoD's information environment. DIEA 1.0 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 DIEA 1.0 to strategically align their programs and architectures with the enterprise net-centric vision. DIEA 1.0 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 DIEA 1.0 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 DIEA 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, DIEA 1.0 will play a key role in transforming the Defense Information Enterprise to net-centric operations.

(This page intentionally left blank)

TABLE OF CONTENTS

Introduction	1
Transformation Context.....	3
Tiered Accountability and Federation	3
DoD Enterprise-level Architectures: Purpose and Scope.....	3
DIEA 1.0 Overview.....	5
Principles, Rules and Priorities	5
Using and Applying Principles and Business Rules	7
Defense 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	16
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)	22
NetOps Agility (NOA)	23
Enabling NetOps Agility	24
Principles and Business Rules	24
DIEA 1.0 Products	26
DIEA Evolution.....	26
The Challenge Forward	27
Appendix A. DIEA Principles and Business Rules.....	A-1
Appendix B. DIEA Hierarchical Activity Model.....	B-1
Appendix C. Acronyms.....	C-1

(This page intentionally left blank)

Introduction

The Defense Information Enterprise Architecture version 1.0 (DIEA 1.0) 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 Defense Information Enterprise comprises the information, information resources, assets, and processes required to achieve an information advantage and share information across the Department and with mission partners. As such, the DIEA 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 Defense Information Enterprise management policy and guidance, including (among others):

- *DoD Net-Centric Data Strategy* (May 2003)
- *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* (Draft Final, March 2007)
- *DoD Telecommunications Policies* (DoDD 4640.13 and DoDD 4650.1, November 2003 and June 2004, respectively)
- *DoD NetOps Strategy* (Draft Final, October 2007)

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 Defense Information Enterprise Architecture 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 DIEA 1.0 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.

DIEA 1.0 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, DIEA 1.0 will directly impact decision making across DoD. Each rule is linked to an underlying policy and/or corresponding standard through the associated activity model. The DIEA will enable decision makers across the Department to have informed discussions on key issues driving the evolution of DoD's net-centric information environment.

DIEA 1.0 will enable decision-makers to have informed discussions on the key issues driving the evolution of DoD's net-centric environment.

By focusing on the "To Be" vision 3-5 years in the future, the DIEA 1.0 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 tiers of the Department – DoD Enterprise, Component, and Program. *Federation* ensures decision makers and implementers understand and align programs and capabilities across tiers. A federated approach allows each tier (in accordance with its Title authority) to leverage the decisions and services of other tiers. Each tier governs the areas for which it is responsible, and should acknowledge and maintain consistency with the guidance from higher tiers. To improve understanding across all tiers, DoD enterprise-level architectures depict department-wide rules and constraints while Component-level architectures depict mission-specific services and capabilities and program-level architectures depict solutions that conform to higher tier rules and constraints.

DoD Enterprise-level Architectures: Purpose and Scope

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

- “What we must do” – a common set of principles, rules, constraints, and best practices that must be followed to meet enterprise goals.
- “How we must operate” – the operational context of the aforementioned principles, rules, constraints, and best practices.
- “When we will transition” - a roadmap (a transition plan) with priorities and strategies for achieving them, as well as milestones, metrics, and resources needed to execute the strategies.

DoD enterprise level architectures typically do not provide implementation guidance or design details for individual systems/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 design principles by enabling each program to filter the 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 DIEA 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.

DIEA 1.0 Overview

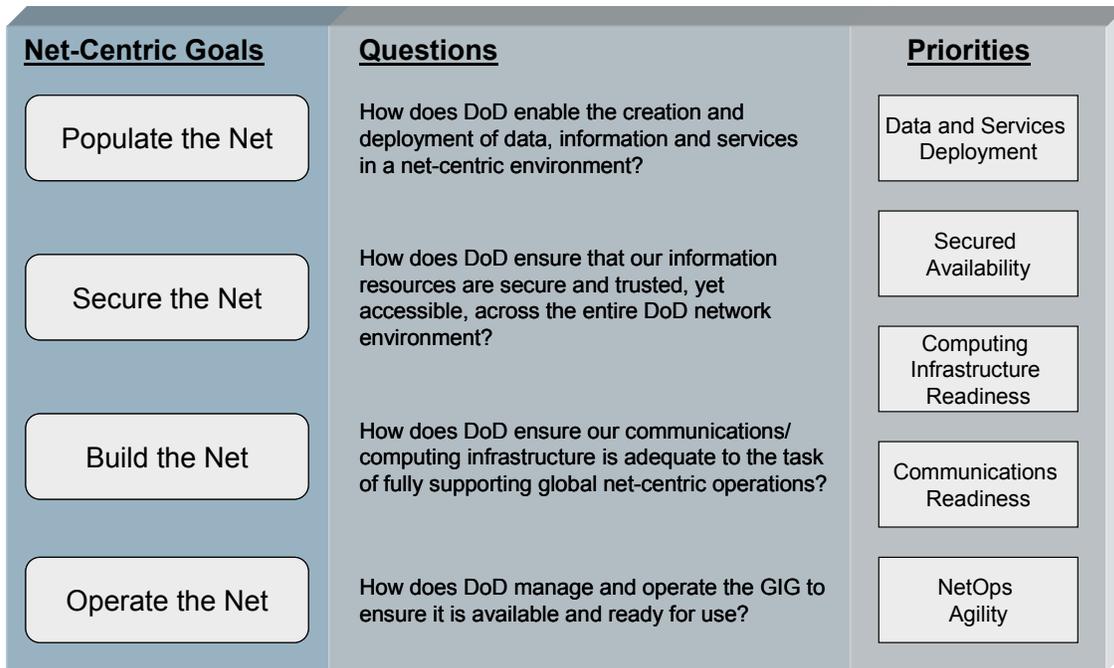
Principles, Rules and Priorities

The DIEA 1.0 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 Defense Information Enterprise 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 DIEA 1.0, 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 DIEA 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 DIEA 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 DIEA must yield to the state of technology, and the needs and imperatives of the Department's missions.

DIEA 1.0 provides context to help everyone from policy makers to system developers understand implications of principles and business rules. Applied pragmatically, the DIEA will drive common solutions and promote consistency and integration across DoD's key programs, applications, and services.

Definition: Defense 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.

Defense 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 Defense Information Enterprise 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 Defense Information Enterprise 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 Department of Defense that enables awareness of, access to or delivers information across the GIG.

- Enterprise Services may be provided by any source within the Department of Defense - 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.

DIEA Products, Evolution, Future Challenges

DIEA 1.0 Products

This initial iteration of the DIEA focuses on establishing a baseline framework of principles and rules that guide the Department's Defense Information Enterprise. Its core product is this architecture description document which:

- Explains the role of the Defense Information Enterprise
- Places DIEA in the context of the Department's Federated Enterprise Architecture
- Establishes Defense Information Enterprise priorities for near-term decision making
- Defines core principles and business rules that should guide all investments

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/cio/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 Defense Information Enterprise 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 DIEA and other DoD architectures for federation purposes.

DIEA Evolution

While DIEA 1.0 represents a strong beginning, it is by no means complete. Given the evolutionary nature of IT development, the DIEA 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 DIEA 1.0 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 DIEA 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 DIEA. 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 DIEA 1.0 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 DIEA 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—particularly the Net-Centric Operations and Warfare Reference Model (NCOW RM) and the Net-Centric Checklist—into the DIEA. This merger, in the next DIEA release, will provide a common, easily understood framework for critical architecture guidance. Additionally, a DIEA compliance guideline document will be developed and published, using the NCOW RM compliance documentation as input.

Achieving the goals of net-centric operations will require sustained commitment across all layers of the Department of Defense. DIEA 1.0 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. DIEA Principles and Business Rules

DIEA 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.
- DoD CIO 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.

Data & Services Deployment Principles

- 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.
- 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 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

- 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 - 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 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 Rules

- 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.
- 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

- 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 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 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 communities of interest.
- 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 shall incorporate flexible, dynamic, non-interfering spectrum use.

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 capabilities for achieving NetOps Agility in Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities.
- 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

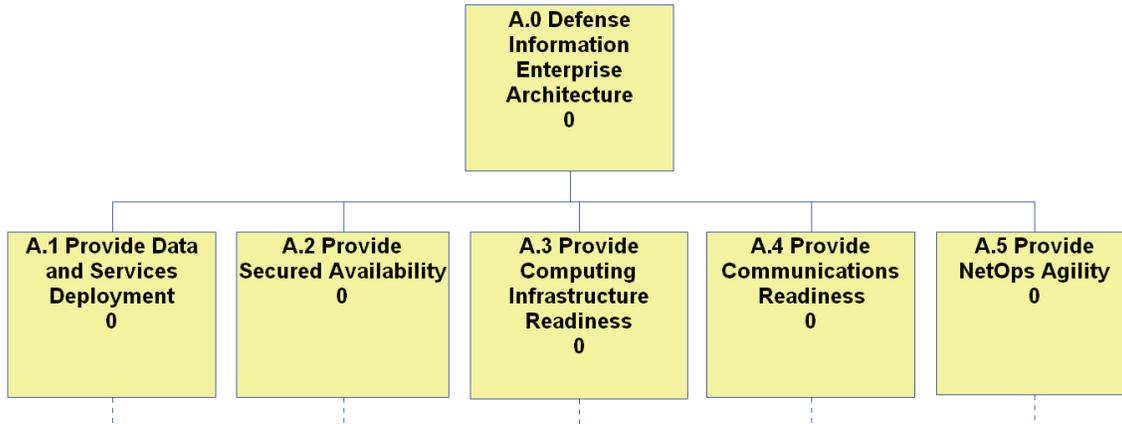
- Share NetOps information with the enterprise by making NetOps data, services, and applications visible and accessible and enable NetOps data to be understandable and trusted to authorized users.

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.

(This page intentionally left blank)

Appendix B. DIEA Hierarchical Activity Model



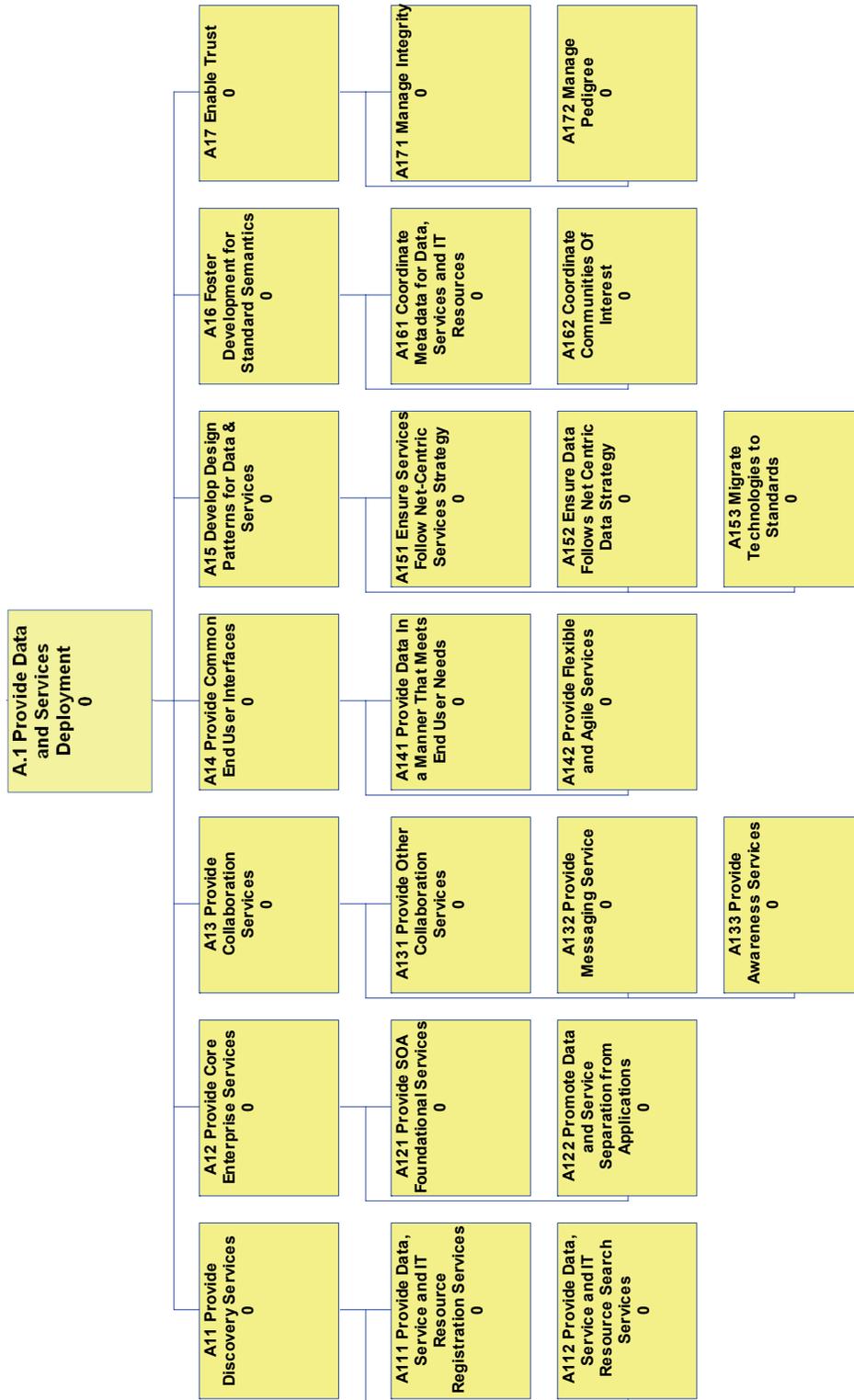
As mentioned in the Executive Summary and Introduction sections, this architecture contains a hierarchical activity model (activity node tree), which decomposes each of the five priorities into a set of core activities performed and/or governed by the DoD CIO. The node tree's five branches represent 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 DIEA 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 DIEA website at: <http://defenselink.mil/cio-nii/cio/diea/>.

- Under the banner *DIEA 1.0 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.

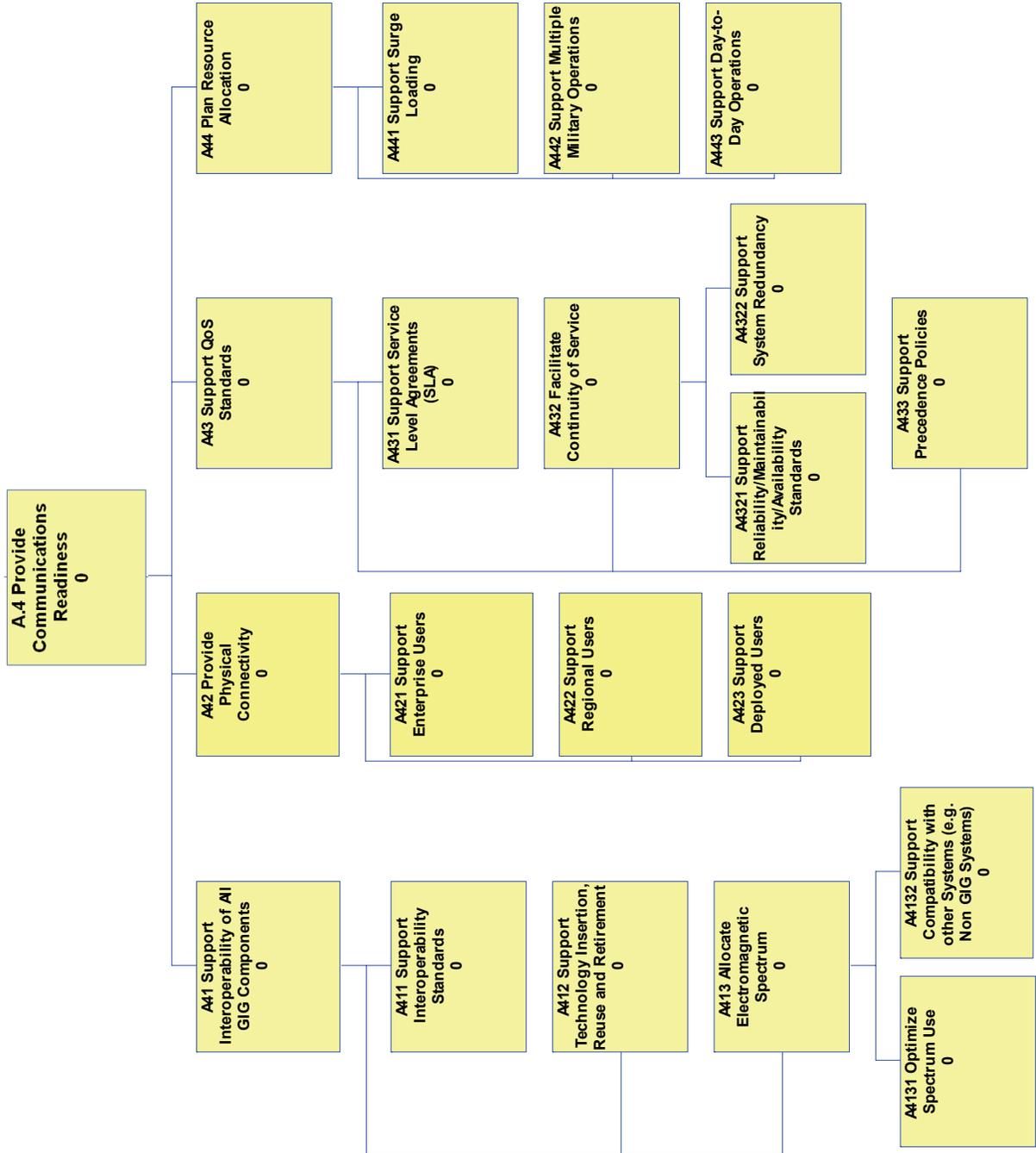
Appendix B Continued: DSD



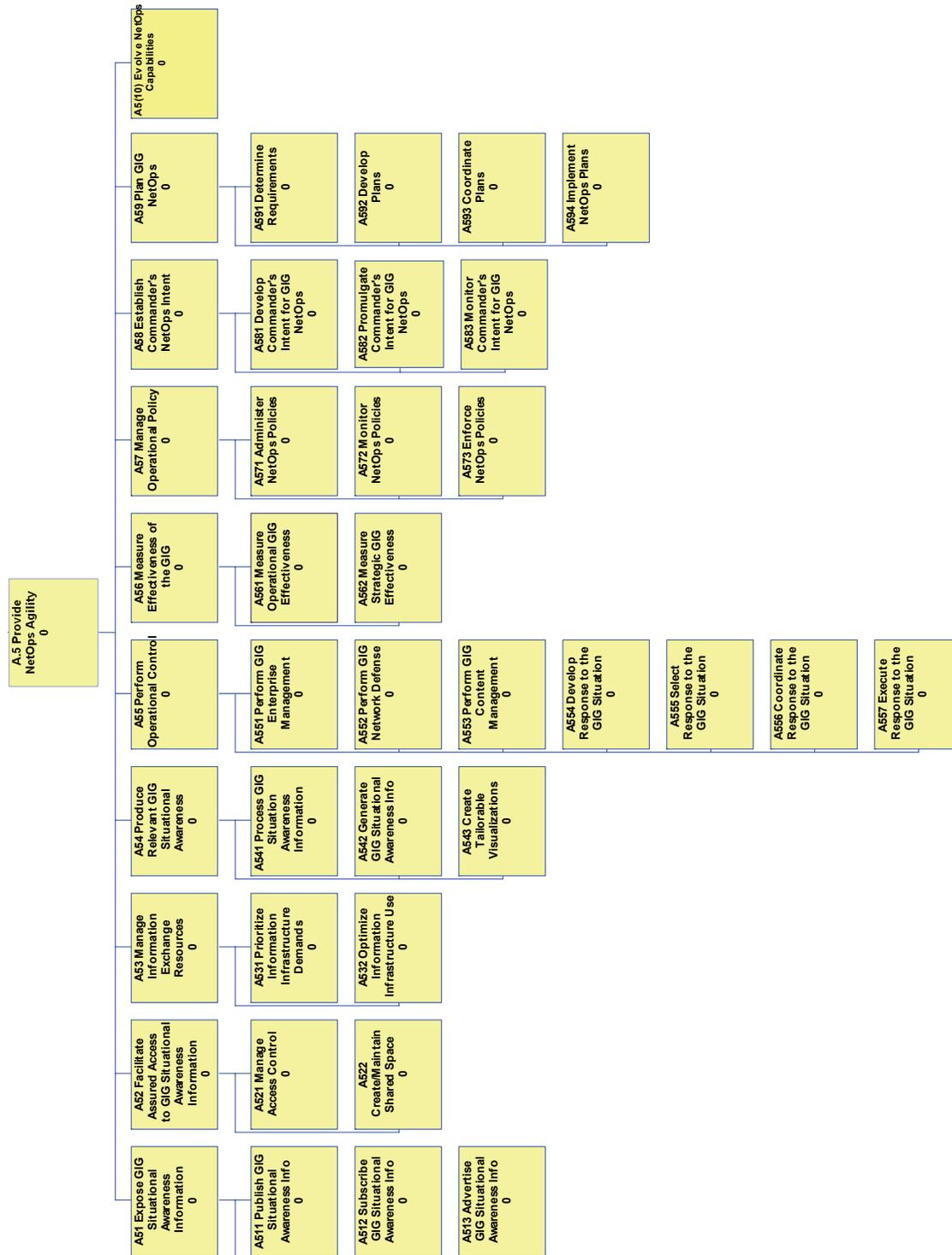
Appendix B Continued: SA



Appendix B Continued: CR



Appendix B Continued: NOA



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
DIEA	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