Department of Defense
Global Information Grid
Architectural Vision

Vision for a Net-Centric, Service-Oriented DoD Enterprise

Version 1.0

June 2007

Prepared by the DoD CIO

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Vision for a Net-Centric, Service-Oriented DoD Enterprise	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense,Chief Information Officer,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**39**	

Table of Contents

List of Figures

Preface

The Department of Defense is transforming to become a net-centric force. This transformation is based upon the recognition that information is a critical strategic component that enables decision makers at all levels to make better decisions faster and to act sooner. Ensuring timely and trusted information is available where it is needed, when it is needed, and to those who need it is at the heart of net-centricity.

Transforming the Department is no small task and will require fundamental changes in processes, policy, and culture. These changes will ensure the speed, accuracy, and quality of decision-making critical to future success. From an information perspective, this transformation is embodied in a dynamic and agile future Global Information Grid (GIG) that enables the Department to fully leverage the power of information and collaboration across the Enterprise to the forward edge of the battle space. The development of the future GIG will eliminate communication stovepipes, meet spiraling information demands, and support unanticipated needs and users. This initial version of the GIG Architectural Vision describes the target GIG.

Our goal in establishing the GIG Architectural Vision is to promote unity of effort among those responsible for evolving today's GIG to its target state, including component CIOs, portfolio managers, and architects. To support this goal, the GIG Architectural Vision is designed to be a short, high level, understandable description of DoD's objective enterprise architecture (required by law and policy). It will be updated periodically to reflect operational, systems and technical changes to the target GIG. Through the development of a series of time-phased GIG Capability Increments, today's GIG will evolve towards the target GIG described in this Vision.

Sincerely,

John G. Grimes
DoD CIO

THE GLOBAL INFORMATION GRID ARCHITECTURAL VISION

Section 1: Introduction

The security challenges of the 21st century are characterized by change and uncertainty. Operations vary widely and partners cannot be anticipated. However, we are confronting that uncertainty by becoming more agile. Greater levels of agility rest upon leveraging the power of information – the centerpiece of today's Defense transformation to net-centric operations (NCO). Our forces must have access to timely and trusted information. And, we must be able to quickly and seamlessly share information with our partners, both known and unanticipated. The GIG Architectural Vision is key to creating the information sharing environment and will be critical to transformation to NCO.

Background

The Global Information Grid[1] (GIG) consists of information capabilities – information[2], information technology (IT), and associated people and processes that support Department of Defense (DoD) personnel and organizations in accomplishing their tasks and missions – that enable the access to, exchange, and use of information and services throughout the Department and with non-DoD mission partners[3]. The principal function of the GIG is to support and enable DoD missions, functions, and operations. Therefore, the way that DoD warfighters, business and intelligence personnel operate must drive the way the GIG is designed, developed, acquired, implemented, and operated.

The current GIG is characterized by organizational and functional stovepipe systems with varying degrees of interoperability and constrained access to needed information. It does not sufficiently exploit the potential of information age technologies, and does not fully support the operational imperative for the right information at the right time. In addition, the current GIG is static rather than dynamic; it cannot quickly adapt to satisfy unanticipated needs and users. Most importantly, the current GIG is not suited to support NCO – it does not support the ability of warfighters and business and intelligence operators to leverage the power of information.

---

1 See DoD Directive 8100.1, GIG Overarching Policy, September 19, 2002, for full GIG definition.

2 In this document, the term 'information' includes the term 'data', as commonly used in the foundation documents used to develop this document.

3 Mission partners are non-DoD individuals and organizations that exchange information with DoD users. Examples include allies, coalition partners, civilian government agencies, and non-governmental agencies and organizations including international organizations.

To support the Department's ever-increasing information demands and future operational concepts the GIG must transform significantly. Part of this transformation will be the way the GIG supports the exchange and management of information and services. The future GIG will enable visibility, accessibility, sharing, and understanding of all information and services among all DoD users, as well as mission partners through well-defined interfaces. A key element of the future GIG will be its ability to extend that visibility, accessibility, and sharing to unanticipated users. The future GIG will provide mission assurance; that is, both information sharing and information assurance on trusted, interoperable networks. As a result, the GIG will support and enable highly responsive, agile, adaptable, and information-centric operations characterized by:

- An increased ability to share information
- Greatly expanded sources and forms of information and related expertise to support rapid, collaborative decisionmaking
- Highly flexible, dynamic, and interoperable communications, computing, and information infrastructures that are responsive to rapidly changing operational needs
- Assurance and trust that the right information to accomplish assigned tasks is available when and where needed, that the information is correct, and that the infrastructure is available and protected

Advances in technology and corresponding innovations in operational concepts and operating practices provide improved information capabilities. These improved information capabilities are the foundation for evolving the current GIG to the target GIG – a dynamic, agile, and robust GIG that meets or exceeds the information requirements of the Department by enabling information and decision superiority.

Purpose

The purpose of the GIG Architectural Vision is to describe the target – and, thereby, provide direction – for the development of GIG capabilities that will support DoD missions, operations, and functions in the future.

The description of the future DoD operating environment and associated GIG capability requirements represent the objective architecture component of the GIG Architecture.[4] **Figure 1** shows all components of the GIG Architecture and the relationship among those components. The DoD Architecture Baseline describes the current DoD environment and the existing GIG capabilities that support operations in today's environment. The DoD Transition Strategy includes an Enterprise-level transition plan built from Mission Area, Joint Capability Area, and DoD Component portfolio transition

[4] The GIG Architecture serves as the DoD Enterprise Architecture. This figure reflects the use of enterprise architectures as defined in OMB Circular A-130.

plans and GIG Capability Increments. The GIG Capability Increments describe future, required operational (warfighting, business, and Defense intelligence) capabilities and the GIG capabilities required to support them. GIG Capability Increments are time-phased as determined by functional owners and GIG capability developers.

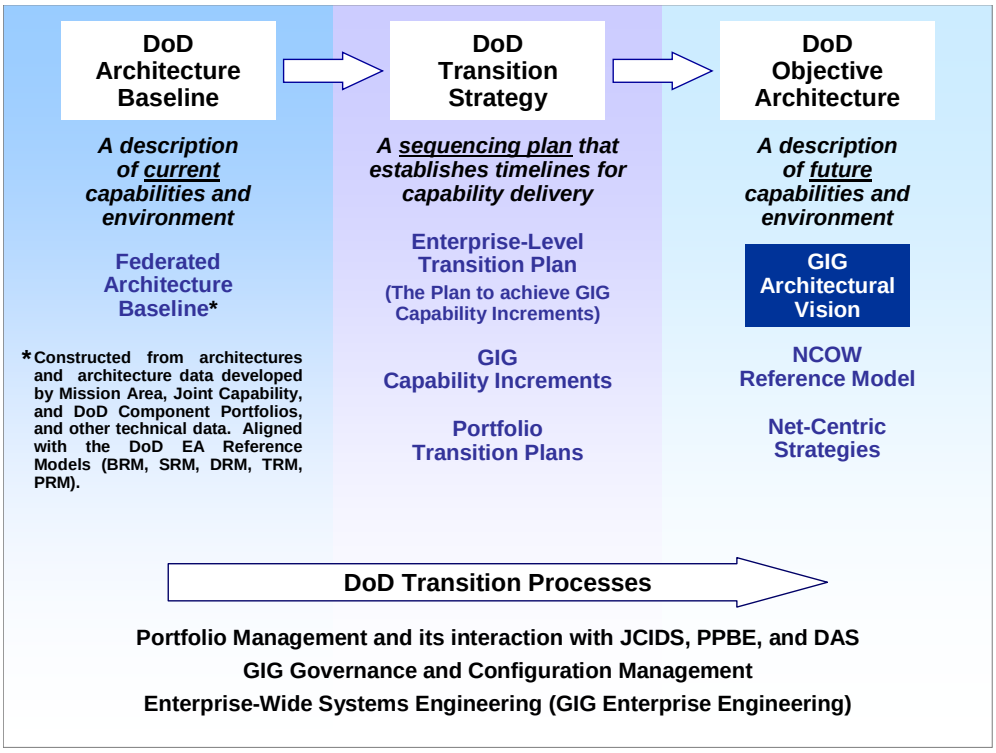

Figure 1 – The GIG Architecture (The DoD Enterprise Architecture)

The GIG Architectural Vision, in combination with other, more detailed descriptions (Net-Centric Operations and Warfare (NCOW) Reference Model and the net-centric strategies), provides the focus for the development of the GIG Capability Increments. **Figure 2** illustrates this concept (with notional dates).

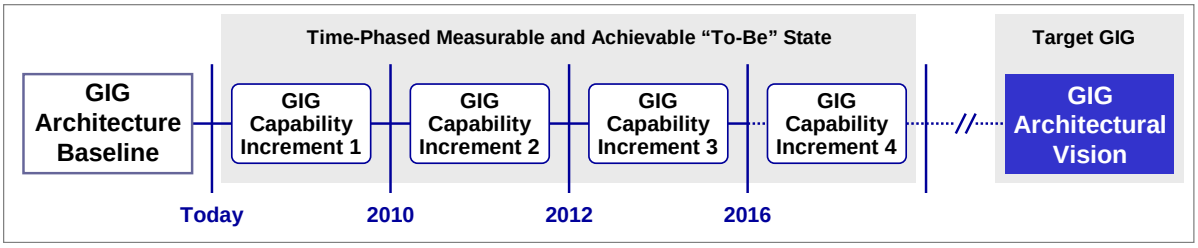

Figure 2 – Transition from GIG Architecture Baseline to GIG Architectural Vision

The GIG Architecture is described through a set of artifacts that document operational activities, information flows, data requirements, services and applications, IT infrastructure, and technical standards.

The GIG Architecture, which is the DoD Enterprise Architecture, is achieved through a federated approach to ensure an integrated, coherent transition to the target GIG through time-phased incremental capabilities. This federated approach applies to the development of architectures at the Department, Mission Area, Component and Program levels and is discussed in more detail in Section 6. The GIG Architecture description provides the detailed information needed to both capture the baseline and define the target envisioned in this document.

Scope and Applicability

The GIG is a federation; that is, ownership, control, or management of the GIG (people, processes, and hardware/software) is distributed throughout the Department of Defense. Similarly, the development of GIG capabilities, guided by a common vision, is distributed throughout the Department. The GIG Architectural Vision provides the common vision and applies to GIG capability development by the DoD Components[5] (including Acquisition Executives, Chief Information Officers, and Portfolio Managers), IT Mission Area Portfolios[6], and Joint Capability Area Portfolios[7]. It should be used to ensure that the GIG capabilities being planned, managed, acquired, and fielded are focused toward a common objective – the target GIG.

This version of the GIG Architectural Vision describes the target GIG, in general terms, from operational, systems, and technical perspectives. It describes a target GIG that is not static but one that is characterized by its ability to rapidly and effectively incorporate operational, systems, and technical change.

Foundation for the GIG Architectural Vision

The GIG Architectural Vision was developed using various DoD documents as its foundation. These documents include:

- Overarching documents
  - The National Security Strategy of the United States of America
  - The National Defense Strategy of the United States of America
  - The National Military Strategy of the United States of America
  - Quadrennial Defense Review (QDR) Report

[5] The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense.

[6] Mission Area Portfolios include the Warfighting Mission Area (WMA), Business Mission Area (BMA), DoD portion of the Intelligence Mission Area (DIMA), Enterprise Information Environment Mission Area (EIEMA), and any new DoD Mission Areas established to manage IT.

[7] Joint Capability Area (JCA) Portfolios include Battlespace Awareness, Focused Logistics, Joint Command and Control, Joint Net-Centric Operations, and any new JCAs established to manage Joint capabilities.

- NCO documents
  - NCE Joint Functional Concept (JFC)
  - Net-Centric Operational Environment (NCOE) Joint Integrating Concept (JIC)
  - Joint Capabilities Document (JCD) for NCOE

- Net-centric guidance and description documents
  - DoD CIO Strategic Plan[8]
  - Net-Centric Data Strategy[9]
  - IA GIG Architecture[10] (includes the GIG IA Strategy)
  - Draft Net-Centric Services Strategy[11]
  - Draft Net-Centric Spectrum Management Strategy[12]
  - Transformational Communications Architecture (TCA)[13]
  - NCOW Reference Model

Other documents such as the Net-Centric Implementation Documents (NCIDs) and the DISA GIG Convergence Master Plan provide valuable technical insight into the target GIG.

The GIG Architectural Vision complements the GIG Technical Foundation with an integrated overview across the multiple modules of the foundation - from operational to technical.

Organization

The remainder of this document is organized into five sections. Section 2 provides an overview of the target GIG and the expected benefits to net-centric warfighting, business, and Defense intelligence missions and operations. Section 3 examines the target GIG from the operational perspective of the user who can be an information consumer, an information producer or provider, or a manager or operator of the GIG. Section 4 describes the system functionality that enables the target GIG discussed in Section 3. Section 5 identifies those technologies that are critical to achieving the

[8] DoD CIO Strategic Plan, Version 1, 2006.

[9] Department of Defense Net-Centric Data Strategy, May 9, 2003; DoD Directive 8320.2, Data Sharing in a Net-Centric Department of Defense, December 2, 2004; and DoD 8320.02-G, Guidance for Implementing Net-Centric Data Sharing, April 12, 2006.

[10] Information Assurance Component of the GIG Integrated Architecture, Version 1.1, 16 November 2006.

[11] Draft DoD Net-Centric Services Strategy (Strategy for a Net-Centric, Service Oriented DoD Enterprise, January 2007.

[12] Draft DoD Net-Centric Spectrum Management Strategy, 3 August 2006

[13] Transformational Communications Architecture, Version 2.0, 31 July 2006.

system functionality of the target GIG. Section 6 addresses the significant shifts in key Defense processes, policies, operational concepts, and culture needed to achieve the target GIG, and includes a short description of the federated GIG architecture concept.

Development Note

This is the initial version of the GIG Architectural Vision. Future versions will be published as required, or within six months following publication of the QDR Report.

Section 2: The Target GIG

The Target GIG Vision

The target GIG vision is for an agile, responsive, and unified GIG that enables the Department to fully leverage the power of information and collaboration across the Enterprise to the forward edge of the battlespace.

Overview of the Target GIG

The target GIG allows all DoD users[14] (and their external mission partners[15]) to find and share the information they need, when they need it, in a form they can understand, use, and act on with confidence; and protects information from those who should not have it. GIG capabilities are effectively aligned to enable a dynamic and responsive end-to-end operational environment, (1) where information is available (2) the means to produce, exchange, and use information are assured and protected; and (3) where resources such as bandwidth, spectrum, and computing power are dynamically allocated based on mission requirements and implemented through the use of precedence, priority and resource allocation techniques. In such an environment, forces, facilities, sensors, decision makers (at all levels), weapons, intelligence analysts, support personnel, etc., are robustly and seamlessly netted together to deliver the power of information out to the forward edge of the battlespace, thereby enabling decision superiority.

The transformation to a target GIG, with information as its focal point, requires fundamental shifts and advances in technologies, architectures, systems, policies, processes, doctrine, and culture. Examples of some key architectural/technical attributes of the target GIG that enable these agile information capabilities and NCO are described in **Figure 3**. These attributes are discussed in more detail in subsequent sections.

Like the Internet, the target GIG's scalable, robust, and highly available communication infrastructure is based on packet switching to interconnect anyone, anywhere, at any time with any type of information such as voice, video, images, or text. With this common Internet Protocol (IP)-based packet communications layer, an information transfer through an EHF MilSatCom terminal to an UHF terminal or to a wired device is transparent to users. Also transparent is an information transfer from an Army brigade to a nearby Marine unit. In the target GIG, technology evolution and system fielding have produced fully meshed networks with managed bandwidth and forward caching to meet the needs of most users, even at the tactical edge. There will always be new

[14] DoD users include information providers and (anticipated/unanticipated) information consumers, whether fixed or on the move, deployed or at fixed installation, human or software/hardware.

[15] Mission partners generally participate through a secure gateway. These gateways permit members to be authenticated, produce and consume information services, and collaborate. However, the GIG and associated services also must allow unclassified information to be exchanged with uncleared civil-military partners outside the boundaries of the DoD Enterprise.

performance and security requirements (driven and derived from technology innovation and operational needs) that cannot be met in the short transitional term by GIG preferred, standard solutions (for instance, the use of higher-performance tactical network protocols that are not compliant with the current version of IP). However, in the target GIG, technical solutions, such as gateways, are provided to maintain information sharing across these disparate networks.

Attribute	Description
Internet & World Wide Web Like	Adapting Internet & World Wide Web constructs & standards with enhancements for mobility, surety, and military unique features (e.g., precedence, preemption).
Secure & available information transport	Encryption initially for core transport backbone; goal is edge to edge; hardened against denial of service.
Information/Data Protection & Surety (built-in trust)	Producer/Publisher marks the info/data for classification and handling; and provides provisions for assuring authenticity, integrity, and non-repudiation.
Post in parallel	Producer/Publisher make info/data visible and accessible without delay so that users get info/data when and how needed (e.g., raw, analyzed, archived).
Smart pull (vice smart push)	Users can find and pull directly, subscribe or use value added services (e.g., discovery). User Defined Operational Picture v Common Operational Picture.
Information/Data centric	Info/Data separate from applications and services. Minimize need for special or proprietary software.
Shared Applications & Services	Users can pull multiple applications to access same data or choose same apps when they need to collaborate. Applications on “desktop” or as a service.
Trusted & Tailored Access	Access to the information transport, info/data, applications & services linked to user’s role, identity & technical capability.
Quality of service	Tailored for information form: voice, still imagery, video/moving imagery, data, and collaboration.

Figure 3 – Target GIG Attributes

In the target GIG, information is considered a strategic, enterprise asset and treated accordingly. The traditional need-to-know policy and cultural model has shifted to a need-to-share model. Like the World Wide Web, the target GIG takes a many-to-many approach to sharing this information. In this case, consider that people both contribute and receive information and information elements are interlinked. The many-to-many approach means that information producers have a means to provide information to many information consumers simultaneously. Conversely, information consumers have a means to access information from many information providers simultaneously. Data assets (including raw[16] and processed data) across the enterprise are visible, accessible, and understandable and can be accessed by anticipated and unanticipated but authorized consumers that ’find and pull’ the information they need in near real-time. A dynamic ‘publish and subscribe’ capability is one way to accomplish this approach.

[16] Raw data are made available at the earliest feasible point in its life cycle to eliminate processing, exploitation, and dissemination delays.

Robust, dynamic IA capabilities are embedded across the target GIG and protect all information, every information transaction, and GIG software and hardware.

The target GIG leverages services and Service-Oriented Architectures (SOAs) to provide access to information and to deliver reusable mission or business functionality as standardized building blocks on an enterprise infrastructure. Services facilitate interoperability and joint operations, support agile delivery of new mission capabilities, and improve information sharing.

The information sharing environment of the target GIG is composed of multiple heterogeneous interdependent elements operating as an end-to-end capability. All entities in the federation operate under a set of enterprise rules. Operation and defense of the GIG is distributed through these federated entities, but decision making is tightly integrated, dynamic, automated, and assured.

The Operational Benefits of Achieving the Target GIG

By globally and robustly networking forces, sensors, users, platforms, applications, information, and decision makers, the target GIG enables net-centric warfighting, business and intelligence missions and operations that leverage the power of information, and support achieving information superiority, decision superiority, and, ultimately, full-spectrum dominance. This dramatically improves information-sharing and command and control capabilities by enabling faster, better decision making, thereby improving the ability of joint forces to operate in environments that are more complex, uncertain, and dynamic. Some examples of the operational benefits this information sharing environment provides include:

- Increased Shared Situational Awareness and Understanding on the battlefield, in business processes, and intelligence operations through near–real-time information sharing and collaboration. Users can relate the information to their particular situations and perspectives; draw common conclusions; make compatible decisions; and take appropriate action related to the overall situation.
- Increased Speed of Command through the real-time availability of quality information for decision making and the ability to rapidly and effectively disseminate direction including the Commander's intent.
- Greater Lethality results from the real-time availability of trusted, reliable information at widely dispersed locations with different classification levels, improved command and control, and enhanced collaboration.
- Greater control of Tempo of Operations by depending on networked environment (and global reach) to support dynamic planning and redirection.
- Increased Survivability through improved situational awareness.
- Streamlined Combat Support by providing users access to the latest, most accurate, most relevant information (e.g., re-supply order status and tracking).

- Effective Self-Synchronization through shared situational awareness, collaboration, and understanding of the Commander's intent.
- Effective Self-Organization of support organizations through shared situational awareness and collaboration, including understanding of the warfighter's changing and present needs.
- Increased Agility & Efficiencies across DoD business operations through interoperability of business systems/applications and establishment of common business services, where appropriate.

Over time, the dramatically improved information capabilities, provided by the target GIG, enable new concepts of operations, new tactics, and new processes/procedures in support of warfighting, business, and Defense intelligence missions and operations.

Section 3: Operational Vision of the Target GIG

This section examines the target GIG from the operational perspective of the users who can be information consumers, information producers or providers, managers or operators of the GIG.

As shown in **Figure 4**, the target GIG supports a wide variety of DoD human and automated information consumers and providers, as well as their mission partners who access the GIG through secure gateways. The target GIG consists of a diverse set of capabilities used for collecting, processing, storing, delivering, protecting, and managing information for these users. The system functionalities that provide these capabilities and the technologies that guide their development are discussed in later sections.

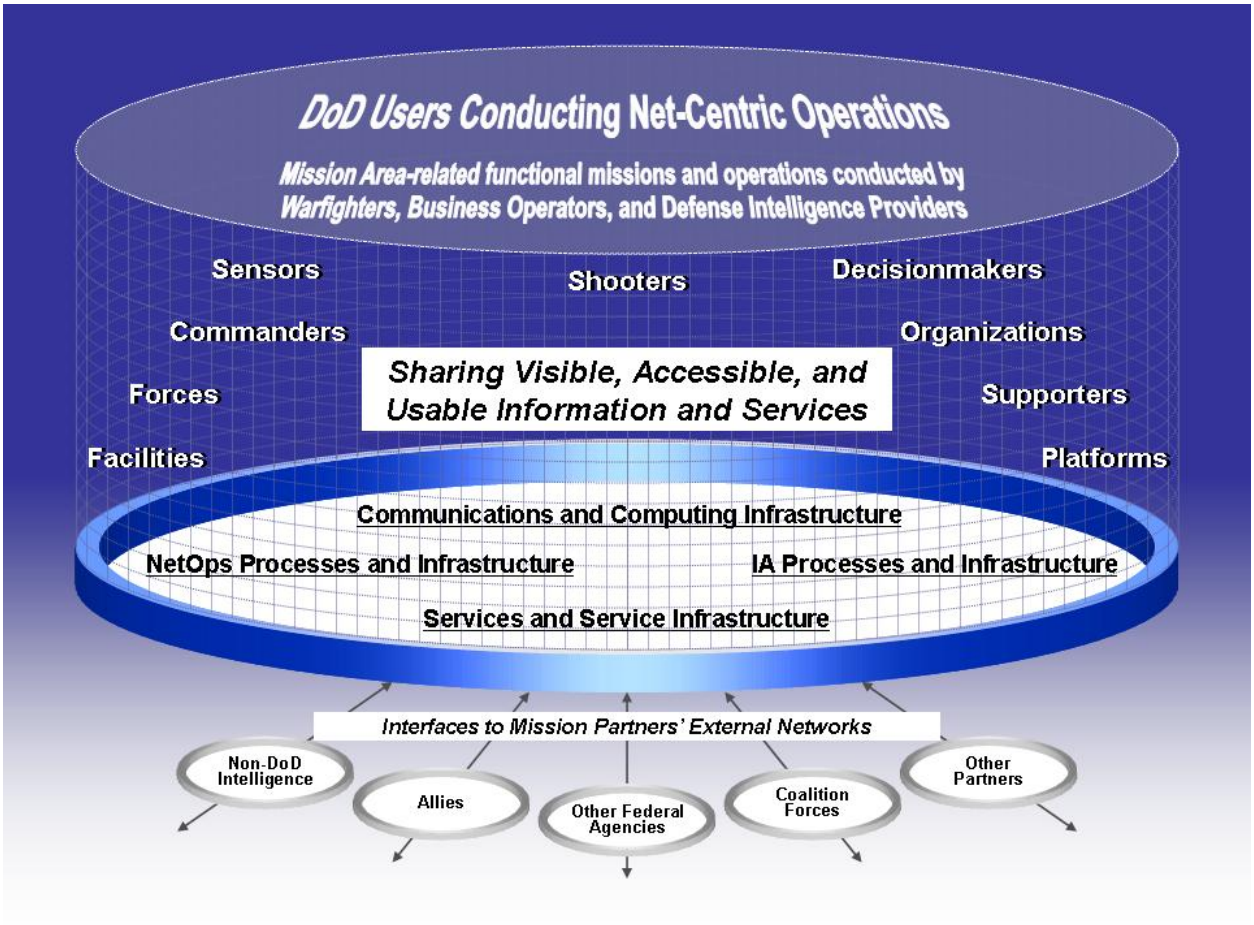

Figure 4 – The GIG and Net-Centric Operations

From a user perspective, access to and use of the target GIG is natural, seamless, persistent, secure and reliable (even under attack) and provides transport, computing and information services at all classification levels. Users can rapidly access the GIG network and remain connected (i.e., be automatically authenticated, recognized, and responded to) as they deploy and move. Even at the tactical 'edge,' users have access

to sufficient bandwidth, that, coupled with network optimization techniques – including information caching and performance management – enables those users to 'pull' or 'post' important bandwidth intensive information such as high-resolution video with acceptable latency. When connections are interrupted and resources constrained, the GIG dynamically adapts service levels (including data compression) and communication paths on a user-priority and precedence basis that optimizes mission assurance.

Figure 5 illustrates information sharing in the target GIG from the perspective of those executing warfighting, business, or intelligence missions. All DoD and Mission Partner GIG users (depicted in the lower part of the figure), with the appropriate authority and trust level, are reliably interconnected to enable them to produce and discover shareable information and services (depicted in the upper part of the figure). Although not depicted in the figure, this shareable information and these services are highly distributed – including being embedded in tactical platforms and user devices. This capability enables geographically distributed users to form dynamic collaborative groups. Access to shared information and services are not restricted by chain of command, location, or network limitations.

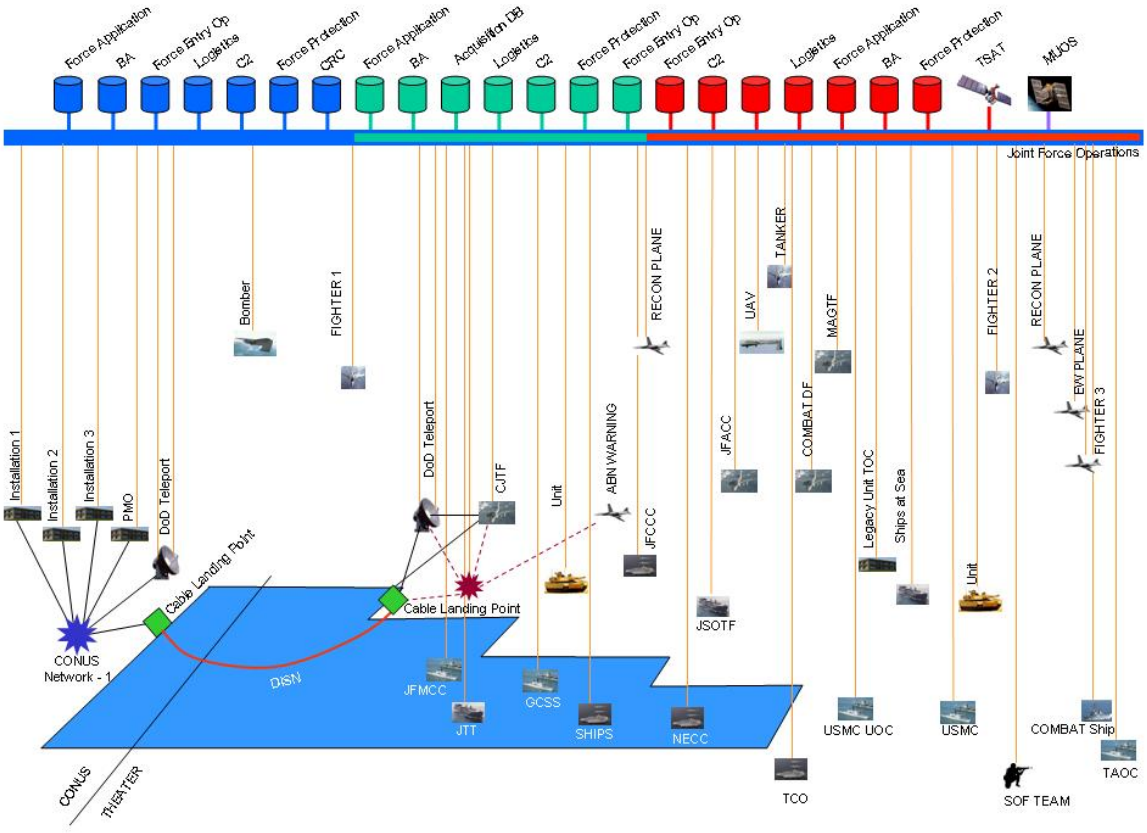

Figure 5 – Information Sharing Within the Target GIG

Information is the key commodity in the target GIG, and vast amounts of data are available in near-real time to information consumers. This includes intelligence, business process, logistics, status, Radio Frequency Identification Device (RFID), sensor, raw, processed, structured, unstructured, and multi-media data. Recognition of

information as a strategic, enterprise asset, coupled with significant improvements in IA and IT capabilities, underlie the willingness of information producers and providers to share information. Data capture, retention, and sharing are key requirements for all new GIG capabilities. Using automated tools, information providers 'post' information to the GIG (so that it is visible, accessible, and understandable to others) as soon as it becomes available. For example, streaming video from an unmanned sensor is 'posted' to the net as it is produced. It is then available to multiple users such as the local tactical Commander and CONUS-based intelligence analysts.

Sharing information is enhanced through a set of automated activities and capabilities including the tagging of information with discovery, semantic, syntax, access control, and other metadata. Metadata is catalogued and discoverable allowing even unanticipated information consumers to find and access the information they need. It is also enhanced by the formation of ad hoc Communities of Interest (COIs) focused on sharing information for specific joint missions/tasks. At a minimum, these COIs agree on a common language and structure for data, and identify relevant information sources. Users can find and access the information they require by advanced search and retrieval methods (pull) or by identifying, in advance, their information requirements (smart pull). Rapidly developed and fielded applications and services (discussed in more detail in Section 4) support advanced, automated methods to fuse, process, visualize, and exploit information in ways tailored to the user needs.

Finally, users explicitly trust the availability, authenticity, confidentiality, non-repudiation, integrity, and survivability of the information, assets, and services of the *assured* target GIG. They also trust the resources that users need to access, share, and use, are not static but can be adjusted to support changing priorities and requirements. GIG NetOps is an enterprise-wide construct that includes procedural and technological elements including doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF). It is used to operate and defend the GIG in support of timely and secure operations and information sharing throughout the DoD and with mission partners. The target GIG is operated and defended as a unified, agile, end-to-end information enterprise that is protected, optimized, and responsive to user needs. Operational GIG capabilities are continually analyzed and provisioned; configurations are controlled; performance is monitored and anticipated; vulnerabilities are mitigated; and resource allocations (including spectrum) are dynamically adjusted to optimize the performance and security of the GIG and meet specific mission demands and priorities.

The next section describes the functions, systems, and services of the target GIG that enable the operational capabilities just discussed.

THIS PAGE IS INTENTIONALLY LEFT BLANK.

Section 4: Systems Vision of the Target GIG

This section describes the system functionality that enables the information-centric GIG discussed in Section 3. As depicted in **Figure 6,** the systems vision of the target GIG is characterized by two major functional components (infrastructure and the mission-specific applications, services and information) that are operated and defended by NetOps to support user needs.

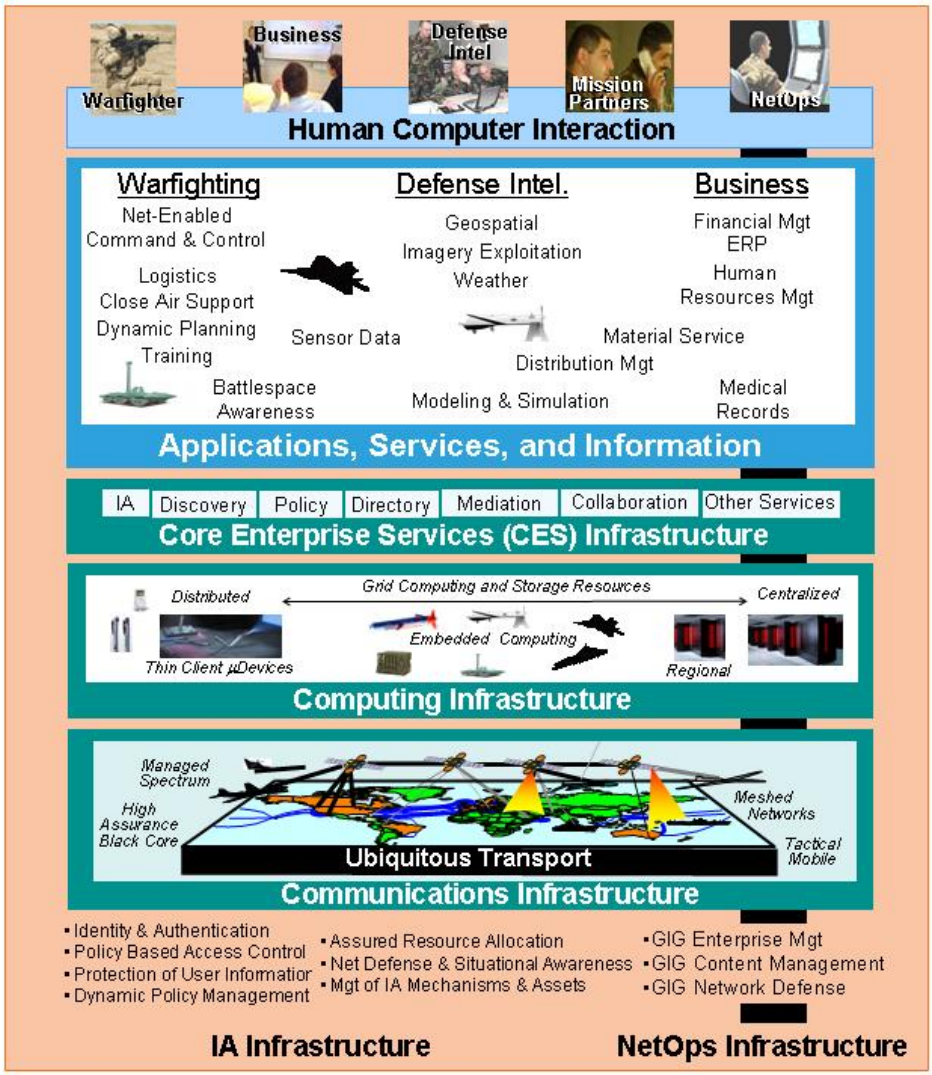

Figure 6 – System Vision of the Target GIG

The heterogeneous GIG infrastructure, globally unified through federation, enables users, including mission partners, to agily transport, store, find, access, process, and secure information across the Department. The communications, computing, Core Enterprise Services (CES), and IA infrastructures of the target GIG are included in the associated domains of the Enterprise Information Environment (EIE) Mission Area (EIEMA) portfolio.

The mission-specific applications, services, and information that use this transparent and robust infrastructure are the second major GIG functional component. It is developed, provided, and maintained by those responsible for the Department's warfighting, business and intelligence missions to leverage the power of information. For example, mission-specific applications and services (such as correlation, fusion, visualization, and modeling and simulation tools), are used (with underlying GIG infrastructure capabilities) to turn sensor and other data into actionable information that can be utilized to plan an operation, target a weapon, task another sensor or order a critical part. These applications, services and information are associated with the Warfighting, Business and Defense Intelligence Mission Area portfolios.

The target GIG's key system functionality is described in more detail throughout this section.

Target GIG Interactions

Human computer interaction (HCI) within the target GIG reflects the highly advanced, natural, adaptive way that humans access and interact with GIG system functionality. This interaction is characterized by highly improved sensory, communications, and cognitive capabilities. Advanced interface technologies, such as sensory augmentation and voice-activation, along with effective training enhance these capabilities.

Automated machine to machine processing of data is critical to leveraging the power of information in the target GIG. Autonomous user agents, applications, and services embedded in weapon or sensor platforms, devices such as RFID and GIG hardware are considered part of the GIG and depicted and implied throughout Figure 6.

Users must be authenticated and authorized. A user's visibility and accessibility to services and information are dependent upon a real-time assurance evaluation of the user's individual transaction requests (transaction-based information assurance). The assurance evaluation considers the trust level of the user role and the quality of protection needed for the requested information as it flows in-transit through the GIG to the user.

Mission partners generally connect to the GIG through a secure gateway from their own networks. Mission partners that are located with a DoD organization may connect directly to the GIG. Mission partners with a direct connection to the GIG may have greater access to information than mission partners with an indirect connection. This is due to the risk associated with communications over an untrusted network path. The access decision will be determined in real time where the level of protection of the network path will be evaluated against the sensitivity level of the requested information and the operational need for that information.

Users normally operate as 'thin clients' using distributed GIG computing and storage resources[17] from the Computing and Communications Infrastructures. In the tactical environment, this mode of operation reduces the risk associated with protection and assurance of information and devices. Users with potential for intermittent or unreliable connection to the GIG, such as tactical users in hostile environments, may be able to operate as a 'thick client' having sufficient resources to locally host and run mission applications based upon service level and assurance policies. In these cases, a user agent periodically connects with the GIG in order to update dynamic information such as user-defined operating pictures, alerts, personal profiles, or updated services.

Applications, Services, and Information

The applications, services, and information depicted in Figure 6 provide the needed system functionality to those engaged in the Department's warfighting, business, and intelligence missions. These services are also used to support EIE capabilities including those associated with NetOps.

Services are extensively used in the target GIG to provide information access and deliver reusable mission or business functionality. Many of these services are based on SOAs. SOA is a way of describing an environment in terms of shared mission and business functions and the interoperable 'building block' services that enable them. SOA supports sharing of distributed internal capabilities with others as well as accessing externally managed capabilities. The Department establishes and enforces how the service building blocks are operated, made available to, and used within the enterprise. Services are supported by the use of a set of common standards, rules, and a common, shared infrastructure.

Systems (including applications) are now largely sets of deployed services cooperating in a given task and orchestrated into complex workflows. These services are adaptable and new capabilities are produced in response to critical DoD warfighting, business and intelligence mission needs. The services available from the CES portfolio (discussed below) provide the SOA infrastructure services and other core capabilities needed for interoperability and access throughout the enterprise. Services in the target GIG facilitate interoperability and joint operations, support agile delivery of new mission capabilities, and improve information sharing.

Services are usually web-based and may be designed to be used by another service (machine to machine) or by a human user (through a user interface). Examples of web-based services that are designed for human use are weather and travel services (e.g., weather.mil and travel.mil). Within the Joint Command and Control community, flexible capabilities such as the Net-Enabled Command Capability (NECC) provide the tailored information needed to make timely, effective, and informed decisions and support the rapid deployment and employment of a Joint Task Force using operationally useful collections of services (some with machine-to-machine interfaces).

[17] These resources may by centralized, such as located at a managed DoD facility, may be dynamically allocated to regional networks, or to local, tactical networks.

Capability providers can build a new application reusing an existing service such as a web service that provides the needed functionality rather than recreating that functionality. Interoperation of disparate applications is simplified by the use of services to facilitate machine-to-machine interactions. Legacy and COTS applications are exposed as services to be discovered and utilized by consumers. The location of these services – the interconnection schemes and infrastructure – and protocols used are transparent to the user. Some GIG capabilities may be large, distributed applications such as modeling and simulation that have service building block components.

All services and information in the target GIG are published to the enterprise (i.e., visible) and are accessible and understandable to the user independent of geography or organization. In addition, all GIG services are assured, which means that the design and implementation of the functionality provided by services provide confidence that security features, practices, procedures, and architecture mediates and enforces the security policy. Assured also means that the provider of the service is validated and that the consumer of the service: can trust the use of services from many different providers, can obtain validated information on the identity of providers, and may be able to negotiate specific performance guarantees in service level agreements. All service providers use a common set of service description information to enable consistent discovery and use of the services.

Services are monitored and managed as part of NetOps. Service consumers will have access to real-time reliability, maintainability, and availability metrics in order to make informed decisions on the reliability of the service for use in mission capabilities. Service providers provide real-time operational status and long-term service-level performance.

Applications still exist in the target GIG. It may not be possible to effectively implement high performance, real-time capabilities using the loosely coupled services approach. However, even in these cases; there are still service-oriented components within the applications, so that information and associated services are visible, shareable, and usable.

Applications and services in the target GIG produce information that must be discoverable, accessible, understandable and useful to consumers. Metadata catalogs exist so that indexed sources of information can be identified, and logical connections to the actual source can be provided, consistent with the responsibility to share and with associated security policies. A search query presented to the enterprise is ‘federated’ to multiple catalogs or indexes to expedite precision searches. To ensure that information is understandable, providers must register semantic, structural, and other metadata in a metadata registry so that automated processes can interpret and exploit data.

The CES infrastructure depicted in Figure 6 and discussed next, provides much of the critical underlying service functionality that enables many of the capabilities just discussed.

Core Enterprise Services (CES)

CES, as depicted in **Figure 7**, are a small set of capabilities whose use is mandated to enable interoperability and increased information sharing within and across Mission Area (Warfighter, Business, Defense Intelligence, and EIE) services. These services enable the secure enterprise-wide interactions between service consumers and providers, ensure that services and information are visible across the enterprise, and are instrumental in enabling SOA implementations to be constructed from services across the enterprise. CES provide SOA infrastructure capabilities such as service and metadata registries, service discovery, user authentication, machine-to-machine messaging, service management, orchestration, and service governance. In the target GIG, other notional examples of CES include candidates such as collaboration and policy services that enable new technologies, protocols and standards that are to be integrated into the existing environment. The CES also include definition and enforcement of the common service standards and rules that ensure networked joint capabilities and interoperability.

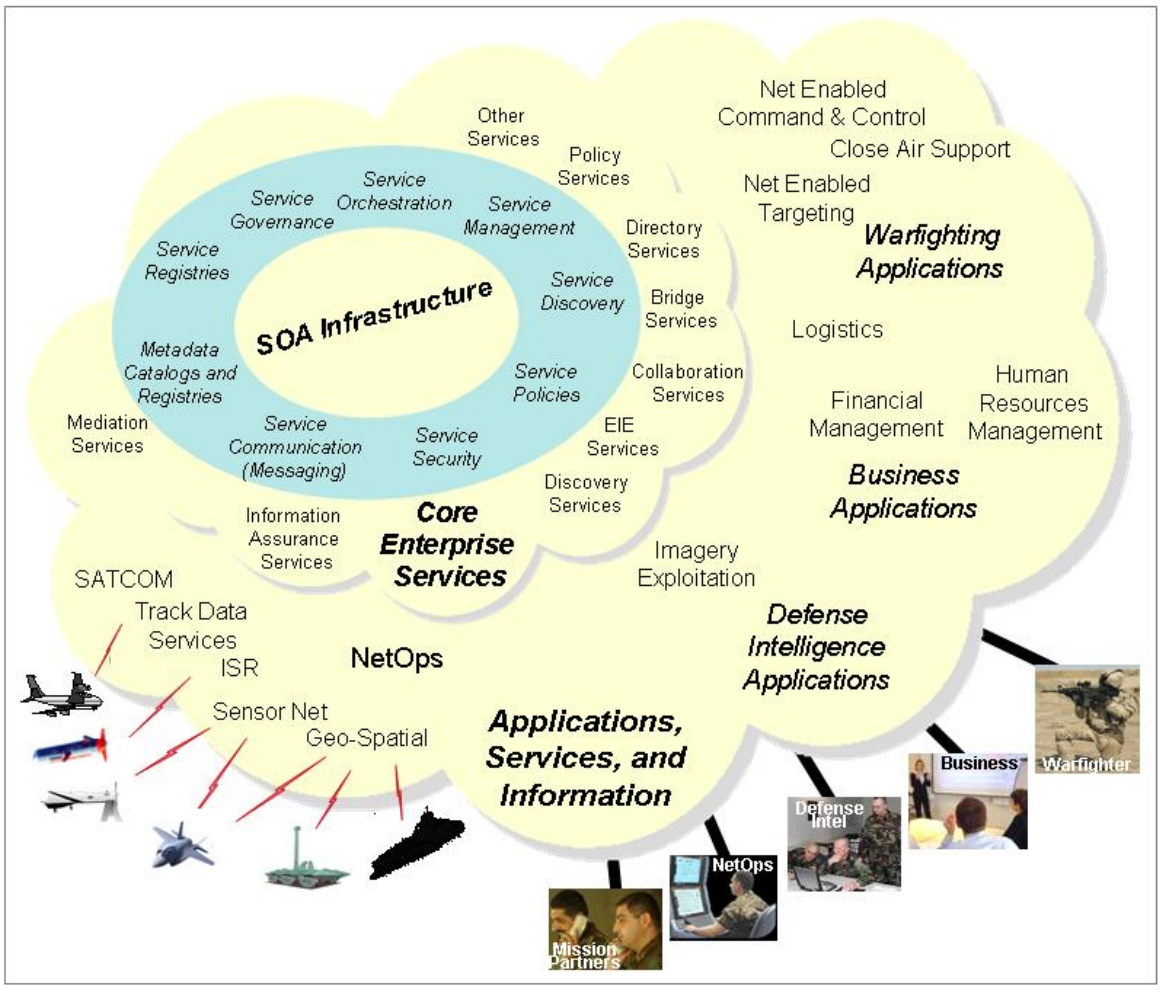

Figure 7 – Core Enterprise Services and the Underlying SOA Infrastructure

The SOA Infrastructure includes a common, shared infrastructure for building services, including core services that enable the development of domain-specific and cross domain applications as SOAs, and enables services to be published and made visible, accessible, and consumable across the enterprise. The core services include IA services that support the necessary assurance capabilities to ensure the widest possible access is supported.

These core services, within the common, shared infrastructure, allow users and information systems to find and bind relevant information, and expose the information they produce (post or publish) for others to discover. The common, shared infrastructure enables the exchange of information among information producers and consumers, while protecting the information from unauthorized access and use.

Information sharing and interoperability in the information-centric target GIG also requires an integrated GIG transport capability. This transport provides mission applications and services with the needed underlying end-to-end, process-to-process, reliable, secure communications spanning all GIG computing and communications resources. As depicted in Figure 6, the computing, communications, and IA infrastructures together with the integrated management, operation and defense of the target GIG (accomplished by NetOps) provide that transport and are discussed in the next sub-sections.

Computing Infrastructure

The assured Computing Infrastructure (CI) (depicted in Figure 6) includes grid computing functionality and assets enabling on-demand, distributed and dynamic, high performance computing. It also includes very large scale data storage, intrinsic support for continuous operations, location independence, distributed execution platforms, operating systems, and all underlying computing platforms and devices. IA data protection applies to data at-rest, in-transit, and in-process.

As depicted in Figure 6, these processing and storage components and solutions vary in technology, architecture, and scale. They range from persistent, service-enabled micro-devices designed with single or multifunction, distributed capabilities (sensors and PDAs, software programmable radios) to tactical, wireless servers and regional and centralized mega-mainframes, and storage area networks. However, to support local and distributed interoperability, a common requirement for all such platforms and architectures is that they are (1) standardized to support common transport, service-oriented and high-performance grid computing environments, and (2) accredited to target GIG assurance standards to be operated and managed by NetOps. In addition, solutions incorporate technology and redundancy to ensure survivability and availability in the face of attacks and failures.

High performance computing and storage area networking provide exponential increases in processing power and distributed storage to enable compute-intensive operations needed to support (1) IA and NetOps (e.g., digital policy execution on a

transaction basis and load balancing) (2) research, development, test, and evaluation communities, (3) large scale operational simulation and modeling and (4) the very large scale data storage capacities needed to capture and process the volumes of data coming from both airborne and land-based sensor nets (estimated to exceed exabytes[18] (10^{18} bytes)).

Grid computing enables the trusted sharing of computing and storage resources across administrative, organizational, functional, geographic, and security domains. Computing and storage resources are monitored and managed as part of NetOps and allocated based on mission requirements.

Parts of the computing infrastructure are operated and maintained by commercial or government computing service providers (CSPs) that provide managed services for hosting and maintaining enterprise services and applications. Managed services provide assured, reliable, and on-demand processing and storage capacity for application hosting, which are governed by Service Level Agreements (SLAs) to ensure adequate performance levels to customers/end-users.

Communications Infrastructure

The Communications Infrastructure (depicted in Figure 6) provides secure, agile, and survivable end-to-end connectivity and on-demand bandwidth that is dynamically allocated, based on operational priority and precedence among millions of space, air, sea, and terrestrial-based fixed, mobile, and moving users. This communications infrastructure supports those on the warfighting edge by enabling (1) the transport of unprecedented quantities of data in and out of the battlefield, (2) global reach, (3) networking on the move (NOTM), (4) reliable delivery, and (5) an ability to dynamically extend connectivity as needed, which includes mission partners through controlled interfaces. It is an infrastructure that users can rely on – one that continues to function under physical, cyber, or electronic attack. Redundancy of paths, the ability to reallocate bandwidth based on path conditions, the commander's policies and priorities, and automated routing alternatives are key to the high availability of this infrastructure.

The communications infrastructure is achieved by integrating the Department's diverse set of communications assets into a reliable, end-to-end communications capability. This integration is based upon adherence to a set of network interfaces, standards, and guidelines in key areas. These areas include: a common network IP, physical communication links, access protocols, routing protocols, consistent Quality of Service (QoS)/ Class of Service (CoS), IA methodologies, capability planning and digital policies.

[18] Large Data Joint Concept Technology Demonstration Program briefing, OSD AS&C, October 2006.

As depicted in **Figure 8**, an IP-based network[19] infrastructure is the foundation of end-to-end interoperability in the target GIG. All types of information such as telephony, multimedia services, video, and data are converged over this universal network.[20]

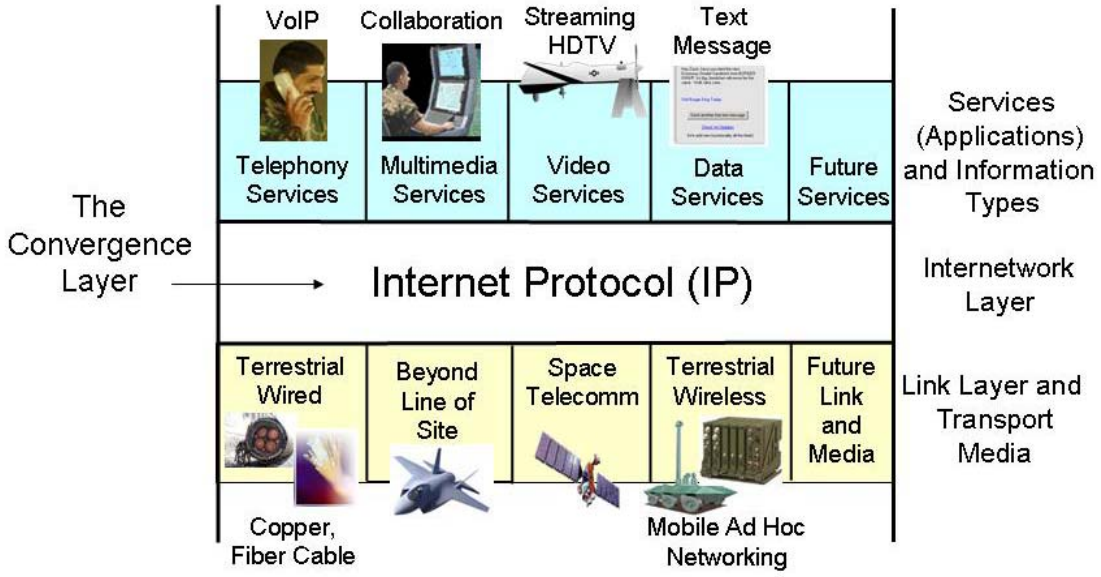

Figure 8 – GIG Internetworking Convergence Layer

Underlying this internetworking convergence layer, all types of DoD-relevant physical transport media and technologies are supported. For instance, this includes copper cable, optic-fiber cable, SATCOM, and tactical wireless (RF and optical). This enables a deployed tactical user to collaborate in real time (without a priori communications planning) with an intelligence analyst in CONUS through mobile ad hoc networks, theater networks, SATCOM, and terrestrial fiber networks (all on a transaction-based, variable trust level).

The IP-based communications infrastructure includes terrestrial, space based, airborne, and wireless segments, instantiated in several key DoD communications programs. **Figure 9** depicts the interconnected nature of these segments in the GIG for DoD users (connections to mission partners are not depicted).

The terrestrial segment provides a ubiquitous, 'bandwidth-available', environment. Most critical facilities are connected with fiber over physically diverse routes using state-of-the-art optical mesh network design. Teleports provide the interface between terrestrial, tactical/theater, and space assets. Tactical gateways and ground stations supplement the Teleports in this interoperability function.

[19] Also referred to as "IPv6 and beyond" to reflect the communications capabilities needed to support the target GIG.

[20] Gateways may still exist between converged IP and tactical environments.

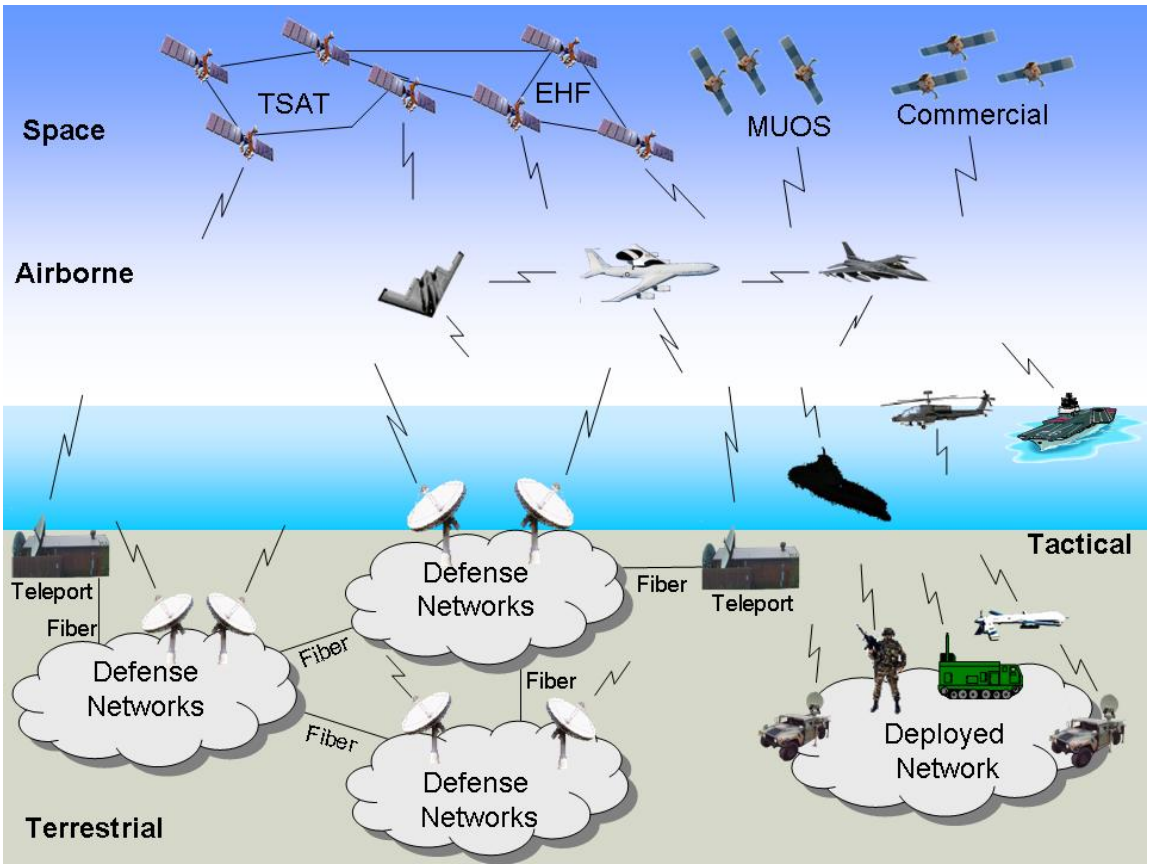

Figure 9 – GIG Communications Infrastructure

The space-based segment includes high capacity, protected, and advanced IP communications equipment such as the Transformational Satellite (TSAT) Communications System that supports IP routing and significant NOTM capabilities in the important UHF and SHF spectrums.

Airborne communications nodes, such as aircraft, UAVs, or tethered air vehicles, provide additional Beyond Line of Site (BLOS) connectivity in theater.

The wireless or radio segment (including handhelds, vehicle mounted, airborne, sea-based, and fixed locations) of the tactical environment is primarily based on software programmable radios such as the Joint Tactical Radio System (JTRS).[21] This family of software-defined radios is programmable to support interoperability and end-to-end routing across divergent networks.

These networks detect other systems operating in the region and automatically set the network or sensor devices to appropriate frequencies. As forces move or other participants join, systems automatically adapt. When two mobile networks overlap, one automatically and seamlessly shifts to a new frequency.

[21] JTRS and TSAT are used here as labels that represent sets of technologies providing expected operational capabilities in the target GIG timeframe. This usage does not presume that these names have permanence in this timeframe.

These communications capabilities of the tactical environment provide continuous BLOS connectivity for most tactical users. Wireless and satellite communications capabilities are the norm and support NOTM with significant bandwidth.

The target GIG communications infrastructure dynamically adapts to rapidly changing conditions, minimizes communications loss, and conserves bandwidth. NetOps monitors and dynamically allocates communications capabilities. Real time, dynamic, electromagnetic spectrum management capabilities and associated policies provide wireless users with 'spectrum on demand.'[22]

Information Assurance Infrastructure

In the target GIG, the Department has evolved from a system-high protection environment to a 'variable levels of trust' protection environment. The vision for this protection environment is based upon the following key elements[23]:

- Transactional Information Protection – granular end-to-end security controls that enable protected information exchanges within the variable-trust Net-Centric Environment.
- Digital Policy-Enabled Enterprise – dynamic response to changing mission needs, attacks, and system degradations through highly automated and coordinated distribution and enforcement of digital policies.
- Defense Against an Adversary From Within – persistently monitor, detect, search for, track, and respond to insider activity and misuse within the enterprise.
- Integrated Security Management – dynamic automated net-centric security management seamlessly integrated with operations management.
- Enhanced Integrity and Trust of Net-Centric Systems – robust IA embedded within enterprise components and maintained over their life cycle.

NetOps Infrastructure

Operationally, the functionality of the target GIG is partitioned into domains. These partitions are derived from operational and technical requirements such as security, organization, function, and geography. These domains are then federated to enable all aspects of assured information sharing and collaborative decision-making capabilities. The target GIG is operated and defended as a unified, agile, end-to-end information enterprise. Centralized direction and decentralized execution of GIG operations and defense enables real time, dynamic responses to critical security and performance issues.

[22] DoD Net-Centric Spectrum Management Strategy, Preliminary Draft, April 25, 2005.
[23] Making the Mission Possible, Net-Centric Environment Information Assurance, Information Assurance Component of the GIG Integrated Architecture, Executive Overview, November 2006, Enterprise IA Systems Engineering Services Office, Information Assurance Directorate, National Security Agency.

NetOps applications, services and information provide real-time situational awareness (SA) and protection of the GIG. Agile and responsive Command and Control (C2) of the GIG provides the ability to effectively respond to unanticipated situations.

NetOps is accomplished through the integration of a set of essential tasks including GIG Enterprise Management (GEM), GIG Content Management (GCM), and GIG Net Defense (GND), and includes all operational aspects of IA. These tasks include:

- Management of the availability and quality of dynamically, varying sets of services
- Flexible and efficient application of globally distributed computing and communications resources including frequency spectrum, communications satellite control, and network management
- Information caching and load balancing
- Dynamic and granular control of embedded security

Protecting and defending the dynamic, distributed, constantly changing target GIG as one virtual capability requires a high degree of automation. For example, in the target GIG:

- The configuration of the entire GIG is managed by software that detects new devices, determines the authorization of any devices, ensures proper configuration and enables and disables all devices with minimal time and effort.
- Digital policy-enabled (pre-programmed and dynamic) network management permits more effective and efficient use of available bandwidth and network self healing, with automatic routing of packets over diverse networks in the event of congestion or outages, enforcement of access, and a range of tailored responses to attacks and vulnerabilities.
- GIG assets automatically provide status, enabling enterprise-wide situational awareness and performance management to GIG-wide service level agreements (SLAs).
- Automated, distributed real-time spectrum management capabilities optimize spectrum use.
- Automated key management and capabilities such as identity, privilege, and security management support operational IA.

This section described the functions, systems, and services of the target GIG. The next section identifies key technologies that enable these functions, systems and services in the target GIG. The relationships among evolving technologies, system solutions, and operational needs are clearly understood and managed in the target GIG.

THIS PAGE IS INTENTIONALLY LEFT BLANK.

Section 5: Technical Vision of the Target GIG

The technical vision of the target GIG identifies a set of complex technologies[24] that are critical to achieving the system functionality of the target GIG described in the previous section. However, technology by itself will not deliver the target GIG; effective use of new mechanisms and methodologies requires major shifts in culture, doctrine, policies, training, processes, organizational roles, etc., as discussed in section 6.

The target GIG is characterized by its ability to rapidly and effectively incorporate evolving technology as well as its drive to seek out technological advantage. This technical vision assumes the high degrees of technology readiness[25] for the targeted technologies and standards necessary to support a robust environment. From a technical perspective, GIG engineers continue to pursue standards-based, multi-vendor solutions primarily based on commercial technology. The NCIDs identifies and addresses these standards-based solutions.

Key target GIG technologies include:

- IPv6[26] technologies (and beyond) that support an assured, reliable, end-to-end, scalable, and survivable mesh transport infrastructure.
- SOA Infrastructure technologies that provide the tools, capabilities, processes, and methodologies to deploy an SOA-enabled DoD enterprise.
- Mobile Ad-hoc NETworks (MANETs) and sensor technologies that support the building of ubiquitous, assured, and agile tactical networks that are federated with the non-tactical domains of the target GIG. Mobile and sensor technologies enable (1) users, appliances, intelligent agents, and other edge devices, wired or wireless; (2) universal access; and (3) exchange of video, voice, and data information of any kind, from anywhere. These networks are self-healing and allow for reconfiguration around failed nodes.
- Human computer interaction (HCI) technologies that (1) address methodologies, processes, and techniques for designing, implementing, and evaluating human computer interfaces, and (2) provide descriptive and predictive models and theories of interaction. The long-term goal of HCI is to design systems that minimize the barrier between the human's cognitive model of what they want to accomplish and the computer's understanding of the human's task.
- Semantic Web technologies that enable user agents to process and share metadata-tagged, actionable information. This includes the automated metadata tagging and discovery technologies that support information sharing.

[24] The target GIG will incorporate these technologies via the associated set of technical, open standards.

[25] Technology Readiness Assessment Deskbook, May 2005.

[26] IPv6 (Internet Protocol version 6) represents a large set of advanced internetworking capabilities that will mature in the target GIG timeframe. IP will require more advanced mesh technologies to reach the reliability expected in the target GIG.

- Ubiquitous RFID tagging for tracking of products, components, and humans throughout the target GIG. As with any GIG capability, the extent that tracking of humans is allowed is governed by law and DoD policy.
- Very large scale data storage, delivery, and transmission technologies that support the need to index and retain streaming video and other information coming from the expanding array of theater airborne and other sensor networks. The target GIG supports capacities exceeding exabytes (10^{18} bytes) and possibly yottabytes (10^{24} bytes) of data.
- High performance computing technologies that will enable the full implementation of Grid computing and services.
- Grid computing technologies that provide support and manage an assured federation of heterogeneous computing, storage, and communications assets available from the GIG infrastructure, and managed as Grid Services by NetOps. The physical characteristics of grid services are generally transparent to users and applications. Grid services provide the necessary qualities of service and protection to enhance NCO. Grid services enable the sharing of these assets across DoD administrative, organization, and geographic boundaries.
- Agent technologies provide autonomous support throughout the Net-Centric Environment (e.g., in applications for disconnected users, tactical users, and enterprise management).
- IA technologies that enable transaction-based access control, information sharing across security domains, protection of information and resources, and maintenance of Situational Awareness in the target GIG.
- Black core enabling technologies that support end-to-end protection of information exchanged among users and services located anywhere in the target GIG. The 'core communications infrastructure' of the GIG is the set of diverse networks and connections owned and managed by different DoD services and organizations. A black core is a set of core components where all data traffic moving among these components is encrypted end-to-end. A black core that extends out to the tactical environment to include user networks and devices will support mobility, security, and survivability in the target GIG.[27] Black core enabling technologies will address, for example, scaleable routing, quality of service, and discovery capabilities that will be provided in the target GIG. Black core supports the evolution of the GIG from a system-high perimeter protection model to a transaction-based Enterprise IA protection model. **Figure 10** provides a conceptual view of an end-to-end GIG with a black core.
- Digital Policy Enabling Technologies. In the target GIG, operational activities, system and service functions, and resources such as applications, services, and networks, are governed by automated rules derived from DoD policy. Automated rules are structured as conditions and actions for managing activities and resources in the context of specific realms such as mission areas, domains, cross-domains, and COIs. An example of a current digital policy-based capability is a network

[27] A. De Simone, J. Tarr, "Defining the GIG Core", draft-gig-defining-the-core-desimone-tarr-051030.pdf, October 2005, www.ietf.org.

management application that dynamically manages IP addresses and QoS at the network level. An example of an emerging digital policy-based technology is Directory Enabled Networking (DEN) which implements policy-based networking to automate the control of large, complex networks.

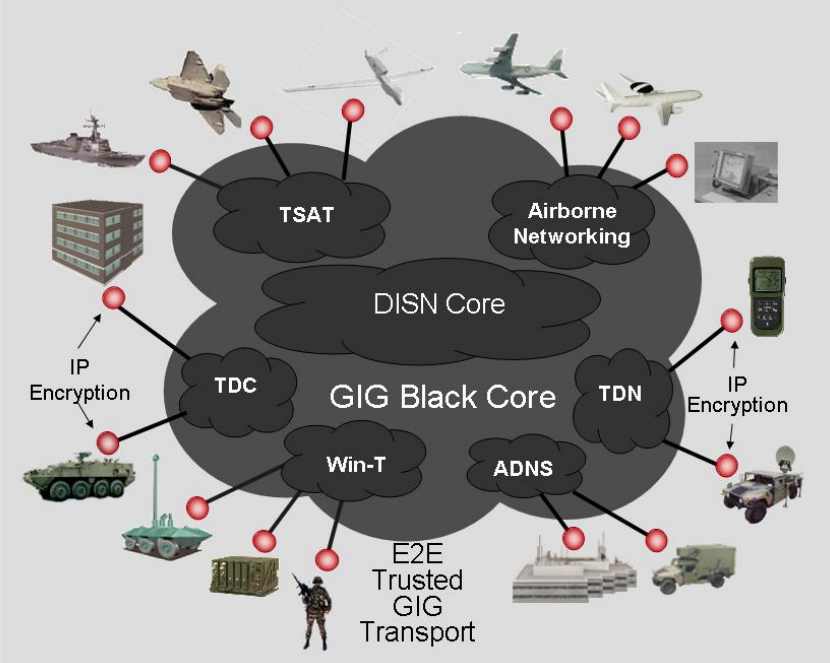

Figure 10 – Conceptual View of an E2E GIG with a Black Core

Innovations in these complex technologies can provide opportunities for either incremental improvements or for major improvements in the capabilities of the GIG. Technologies that enable incremental improvements have a relatively small impact on elements of DOTMLPF. These are called *sustaining technologies* and examples typically include new releases of operating systems, and processor and memory technologies that double processing speed and memory size every two years.

Technologies that enable major or radical improvements to existing capabilities may have a relatively large impact on elements of DOTMLPF. These are called *disruptive technologies*[28]. Past and current examples include the telephone, the computer, the electronic spreadsheet, the PC, the World Wide Web, the cell phone and the iPod.

The complex target technologies identified above contain both sustaining and disruptive components. As the Department has effectively integrated the benefits of disruptive technologies such as the World Wide Web, it will also effectively integrate the benefits of the disruptive components of these target technologies in the future.

[28] See "The Innovator's Solution," Clayton M. Christensen, 2003 and the body of related academic work on technology innovation.

An example of an expected benefit (capability) to be obtained from integrating elements of these target technologies into the target GIG is a wearable, hands-free computer system. This system will be embedded in clothing, and integrated with trusted, reliable, battlefield communications. It will host advanced technology applications that are consistent with this vision of net-centricity and service-orientation. Hands-free computer interfaces such as eyeglass video monitor lenses, retinal scans, and voice recognition will enable increased automation and multitasking. The system may have a trusted user agent capable of logging into the GIG to provide continuous health monitoring and obtain updates to user-defined operating pictures (UDOP). The delivery of this capability will be dependent upon innovations spanning the current (and future[29]) target technologies.

Technologies will continue to increase in complexity. Innovations will occur with greater frequency and be adopted in shorter time frames. Continued Department-wide early value determination and adoption of technologies, along with the co-evolution of technologies and operational capabilities, is essential for evolution to the target GIG.

The next section discusses the transformation necessary for achieving the target GIG and beyond.

[29] The Global Technology Revolution 2020, In-Depth Analysis, Rand Corporation, 2006.

Section 6: Achieving the Target GIG

Achieving the target GIG involves successful transformation in terms of the people, processes, and technologies comprising the GIG. Investments in new capabilities, replacements, or gateways for legacy capabilities, and upgrades through technology refreshments, do not by themselves achieve the vision of an agile, information-empowered Defense enterprise. Significant shifts in key Defense processes (e.g., JCIDS, PPBE, DAS, and T&E), policies, tactics, operational concepts, and culture are critical. At the same time, the goal is to maintain and improve IT acquisition efficiency and operational effectiveness, with an emphasis on supporting the warfighter.

A key IT transformation is the shift from static mechanisms for allocating, operating, and defending IT resources (e.g., spectrum, bandwidth, computing power) to dynamic, automated, mechanisms. The GIG Architectural Vision does not assume unlimited IT resources in the future, but envisions dynamic allocation of resources based on changing user needs, cyber threat, and mission priorities. Cultural, policy, and process shifts; operational/mission leader championship; as well as experience and training are important in fully and confidently achieving these capabilities.

Ensuring that relevant information is readily accessible requires a fundamental culture shift within the Department. This shift is underpinned by changes in policy, training, doctrine, organizations, operational concepts, processes, and visionary leadership. In the target GIG, information producers recognize that their information is a strategic, enterprise asset to be shared to the fullest extent possible. This includes widespread acceptance and practice of tagging and posting information in parallel with its processing and analysis. The traditional need-to-know model (based on an information producer's determination of who needs to know) is changed to a right-to-know and need-to-share model, while still protecting the information through robust, dynamic IA capabilities. Cross-domain and cross-organizational COIs are established, resourced, and empowered – to ensure that shared information is understandable – by agreeing on common syntax and semantics (vocabularies) where most needed. Furthermore, in the target GIG, information producers and providers are widely valued for their contributions and incentivized to contribute. For example, the accessibility, accuracy, and utility of the information provided are key factors in GIG investment and sustainment decisions.

Significant cultural, policy, and process changes are needed to ensure that the target GIG is net-neutral, global, and end-to-end. For example, an Army analyst may use available Marine computing assets to process intelligence information using visualization and fusion services provided by the National Geospatial-Intelligence Agency. In addition, acquisition, PPBE, and capabilities processes evolve to incentivize the development, acquisition, operation, and sustainment of the needed capabilities. Effective and collaborative architecting, systems engineering, testing and evaluation, and portfolio management of GIG capabilities (vice individual systems/programs) drive these processes and provide an integrated, coherent transition to the target GIG through time-phased incremental capabilities.

The federated DoD Enterprise Architecture (EA) is a key element in achieving this transition. This approach provides an enterprise-wide common lexicon to support the numerous decisions related to strategy and IT investments needed for success. The federated DoD EA exists as a set of architectures that are linked and aligned via mission, function, and domain taxonomies from the DoD Reference Models (RMs). Individual contents are accessible, visible, and understandable to DoD process decision makers, including those operating and defending the GIG. The DoD EA provides the single source for descriptions of operational processes, GIG Capability Increments, and current and planned IT investments to realize those Increments. It also provides the analytical data source for investment decisions. Enforcement, through architecture governance and existing processes, is the key to success. The vision for architecting the target GIG is a federated architecture approach. **Figure 11** is a notional example of architecture artifact distribution throughout the federated architecture.

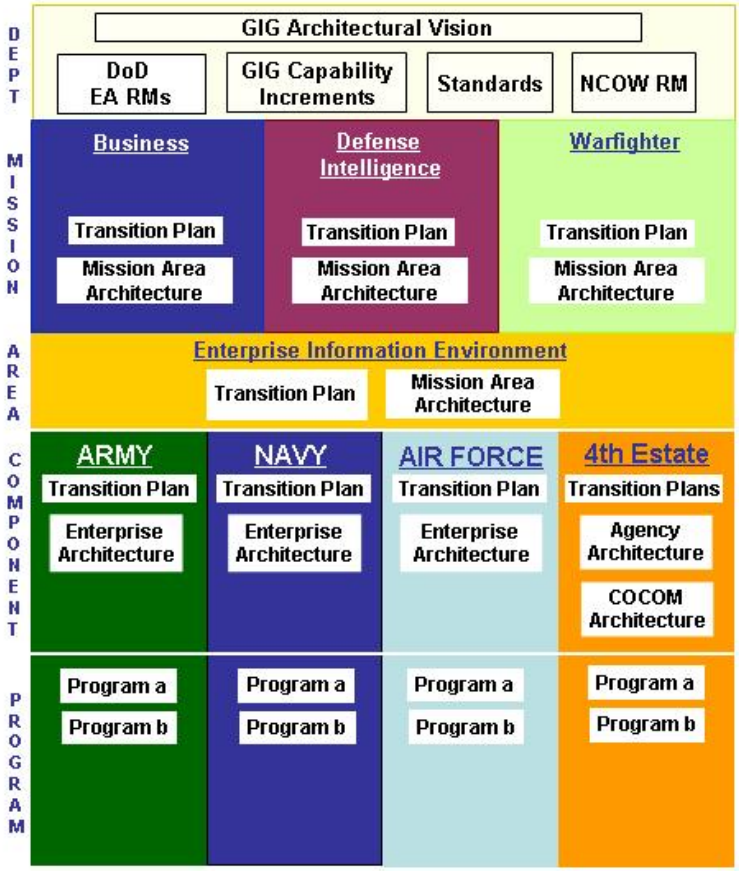

Figure 11 – GIG Federated Architecture Approach (Notional)

This federated architecture approach is described in more detail in the Draft Version 1.01 of the DoD EA Federation Strategy, 4 December 2006. This approach provides a framework for enterprise architecture development, maintenance and use that aligns, locates, and links disparate architectures and architecture information via information exchange standards to deliver a seamless outward appearance to users. This

federated architecture approach recognizes the uniqueness and specific purpose of disparate architectures and allows for their autonomy and local governance while enabling the enterprise to benefit from their content. Authority, responsibility, and accountability for producing these architectures are distributed throughout the Department. As depicted in Figure 11 these tiers represent the Department, Mission Area, Component, and Program levels and contain architecture content specific to that level. A Federated Architecture aligns activities, services, systems, and infrastructure with federation standard taxonomies. They also conform to a common context established by rule sets or mappable standards across autonomous Mission Areas, DoD Components, and Programs, thereby minimizing the uniqueness among these autonomous elements. Artifacts are federated (semantically aligned using common mappable elements) to provide an overall view of the enterprise and are made accessible, visible, and understandable to DoD process decision makers, including those operating and defending the GIG.

GIG federation across all DoD Components and with mission partners is critical to achieve a collaborative information sharing capability. This capability must support all phases of conflict, as well as humanitarian assistance and disaster relief. In the target GIG, policies and processes to support this federation – and the ability to dynamically establish appropriate organizational relationships – are in place. Some processes (e.g., Certification and Accreditation, Configuration Management) evolve to better reflect the integrated nature of this target GIG. Information for emerging and existing GIG capabilities will be available and shared through enterprise-wide implementation of the DoD Net-Centric Data Strategy (in concert with the architectural approach just discussed). Cultural change is also essential to effectively operate in this environment, as individuals and organizations maintain flexible, authoritative relationships.

Finally, realization of the operational benefits of the target GIG in enabling NCO requires the development and implementation of new concepts of operations, tactics, business processes, and organizational changes for the Department. Training and experimentation are critical in identifying and validating the benefits and risks of information sharing, as well as its impact on NCO. To promote the desired cultural change and ensure the proficiency of net-centric skills, continuous training is essential for developing an individual's knowledge, skills, and abilities to function in the environment enabled by the target GIG.