Office of the Assistant Secretary of Defense for
Networks and Information Integration/DoD Chief Information Officer

Global Information Grid Core Enterprise Services Strategy

DRAFT

Version 1.1a

Production Date: 7/9/03

This document and a commenting mechanism are available at the Global Information Grid (GIG) enterprise services (GES) portal at:

http://ges.dod.mil

The Points of Contact (POC) for this document are:

Geoff Raines
Graines@mitre.org
703-883-7946

Rob Vietmeyer
VietmeyR@ncr.disa.mil
703-882-0566

1 Introduction

The Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) has articulated a vision for transformation of the information environment in the Department of Defense (DoD), calling for a move from the centralized thinking and planning currently reflected in the Task, Process, Exploit, Disseminate paradigm, to an edge-centered Task, Post, Process, Use (TPPU) approach to information sharing and availability. The envisioned changes represent a fundamental shift to a service-oriented paradigm which requires the support of a ubiquitous network environment, richly populated with information of value, as determined by the consumer, which is highly available, secure, and reliable.

Robust Global Information Grid (GIG) enterprise services (GES) will provide visibility and access to data, enabling the end user to execute an intelligent pull of mission-tailored information from anywhere within the network environment. Users will see a collection of GES networked capabilities organized as Core Enterprise Services (CESs) and Community of Interest (CoI) services. The CESs provide the basic ability to search the DoD enterprise for desired information and services, and then establish a connection to the desired service/data.

A new program called Net-Centric Enterprise Services (NCES) has been proposed to provide the services and capabilities that are key to enabling ubiquitous access to reliable decision-quality information. The scope and requirements for GES are being defined through an Analysis of Alternatives (AoA), which will provide recommendations and details necessary to support an NCES Milestone B decision currently scheduled for 2nd quarter FY2004. In support of the AoA activity, an initial set of core enterprise services has been identified and is being further defined by inter-Service, inter-Agency teams.

1.1 Purpose

This document defines each of the CESs, describes the technical capabilities that will be delivered by the CES, and presents a strategy for evolution of capabilities from an initial baseline through FY2008. The detailed definition of the CESs in this document will support the AoA Study Group and its supporting technical working groups in definition and analysis of GES alternatives.

Making DoD's net-centric environment operational will be achieved in part by using the capabilities and tools that exist today and implementing knowledge, processes, people, and technologies to raise the level of enterprise services offered to customers of the enterprise. The CESs that the GES will provide to DoD will evolve from current capabilities offered by existing systems and Programs of Record (POR) operating throughout DoD. The information presented in this document will enable the dialog necessary to begin identification of the current systems and POR that will develop and evolve the envisioned capabilities at the enterprise level.

Migration to the desired net-centric end-state will take several years. While CESs are being developed, all Command and Control (C2), Combat Support, and Intelligence Systems supporting the Joint Task Forces (JTFs) and Combatant Commands will continue to use and implement the common operating environment (COE) where applicable, and will be required to define transition plans and approaches for migration from the COE to mandated CESs. The definition and evolution plans for CESs presented in this document will assist in the development of transition plans for users and developers of current capabilities, in accordance with transition planning guidance to be issued by Acquisition, Technology, and Logistics (AT&L), NII (CIO) and the Joint Staff. DoD business systems will also use the CESs, and this document will help the business programs plan accordingly.

1.2 Scope

Implementation of GES will be achieved via an evolutionary approach, where "increments" of capabilities will be defined and associated with target implementation dates, and underlying technical components will be allowed to evolve toward those target capabilities on a cycle keeping with current technology innovation and operation cycles. This underlying technical evolution, referred to as "spiral evolution" will be aimed at achieving flexibility and accelerating fielding and adoption of new capabilities necessary to support the warfighter while achieving information superiority.

This draft of the document focuses on providing detailed definition of Increment I capabilities for core enterprise services, to be achieved by the end of FY 07. Where feasible, it also provides the definition of capabilities beyond Increment I, in order to establish a more comprehensive vision of the direction of core enterprise services.

The Increment I services are described herein in terms of capabilities, without dictating architectural or technical implementations. This is in keeping with the overall approach for technical definition of Increments and Spirals, as follows:

- A capability strategy for a given increment (*Increment n*) is defined, setting forth the target capabilities and timeframe when the capabilities should be fielded.

- *Increment n* architecture is developed, in accordance with GIG Architecture Framework constructs.

- Cognizant Program Offices oversee the development and fielding of incremental capabilities leading up to the target, in step with technology innovation, operation cycles, and resource availability, including research and development of new concepts and technologies via concept exploration pilots, Advanced Concept Technology Demonstrations (ACTDs), and funded research.

- At completion of *Increment n,* the capability strategy is revisited to provide further definition for *Increment n+1,* allowing for necessary adjustments due to strategic, technical, operational, or programmatic changes.

2 Background

The figure depicts the broad scope of GIG Enterprise Services (GES). As the enterprise services component of the Global Information Grid, GES is the infrastructure on which DoD computer applications (eg.C2, Combat Support, Medical) rely. GES in turn relies on the GIG transport services such as the Defense Information System Network (DISN) and tactical communications systems. DISN and tactical communications systems consist of transmission systems, distribution/switching systems, Video Teleconferencing (VTC) and packet and other support infrastructures. While GES relies upon the GIG transport services for the exchange between the Core Enterprise Services (CESs) and the Community of Interest (CoI) capabilities, transport is not an inherent component of GES.

- **GIG requires a common set of information services to provide the awareness, access and delivery of information.**
- **GIG Enterprise Services (GES) is a collection of networked capabilities organized as Core Enterprise Services (CES) and Community-of-Interest (COI) services.**
- **CES, generic information services that apply to any COI, provide the basic ability to search the enterprise for desired information and then establish a connection to the desired service.**
- **COI's are organized around DoD, IC, and dynamically created communities that have similar information requirements**

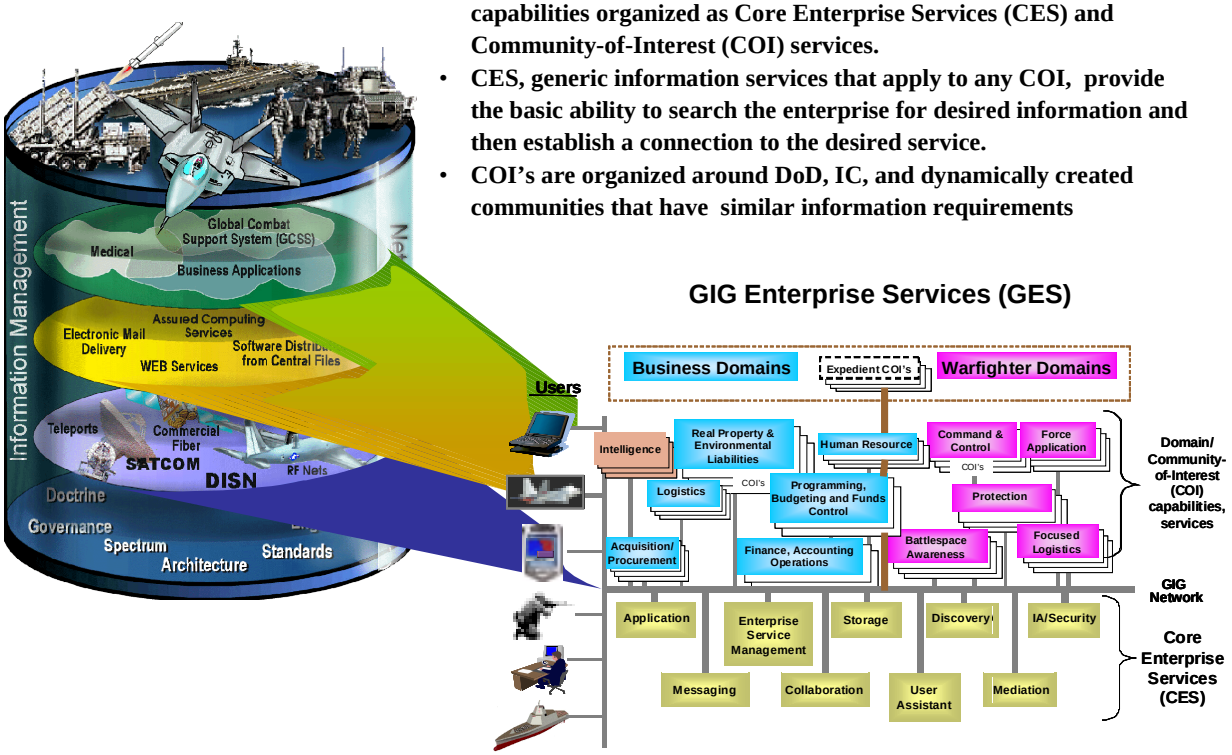


Figure 2-1 Core Enterprise Services for the GIG

Service As An Architecture Concept

A formal definition of service is "A service is a contractually defined behavior that can be provided by a component for use by any component, solely based on the interface contract." To apply that in the context of the GIG, we can draw from the telecommunications and information services industries to define enterprise services as "a meaningful set of capabilities provided by a system (or set of systems) to all who utilize it" (TINA 1997). This may include telecommunications or network transport services, services that handle information resources including the storage, retrieval, manipulation and visualization specific to the resource, and management services including fault, configuration, accounting, performance and security functionalities, as well as service lifecycle management, service instance management and user life cycle management. (TINA 1997)

The Joint Requirements Oversight Council (JROC) approved GIG Capstone Requirements Document establishes the need to provide a common set of information capabilities for the GIG. The current GIG Architecture (GIG Architecture v2) defines the information environment that the common set of information capabilities (or GIG enterprise services) must support. The DoD information environment is moving from broadcast and point-to-point communications to a net-centric environment. This new environment must (1) support posting data to public spaces as early as possible; (2) provide users with the capability to pull whatever they want, whenever they want, from wherever they are; and (3) ensure security. GIG enterprise services must support the entire DoD and Intelligence Community (IC), conventional and nuclear warfighting, and business units.

Community Of Interest Services

The basic characteristics of Communities of Interest (CoIs) have been identified in the DoD Net-Centric Data Management Strategy. The CoIs are collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes, and who therefore must have shared definitions for the information they exchange. Communities provide an organization and maintenance construct for data, operational processes and mission capabilities, providing boundaries to group information and functions relevant to the CoI. CoIs may be composed of members from one or multiple functions and organizations. Institutional CoIs, whether functional or cross-functional, tend to be continuing entities with responsibilities for ongoing operations. They also lend support to contingency and crisis operations. Expedient CoIs are more transitory and ad hoc, focusing on contingency and crisis operations. In all cases, the information and the functions that operate on it are bounded by the CoI. This implies a tighter coupling of information and functions within a CoI, and a looser coupling between CoIs.

Each CoI service will provide or support a well defined set of mission functions and associated information. The services will have an access point that defines how to access its functionality and data. A CoI service may not provide all of the functionality required to realize a CoI mission or process, and a combined set of services may be required to interact to achieve the complete solution. The set of CoI services will provide a CoI with a 'toolbox' to build solutions for their specific challenges.

Core Enterprise Services

Core Enterprise Services (CESs) enable both service and data providers on the "net", by providing and managing the underlying capabilities to deliver content and value to end-users. CESs have to support a broad array of services and should be open to allow the introduction of new classes of services. The CESs should be able to support new requirements and CoI needs without re-engineering and re-implementation. To enable the support of NCW, the CESs must support the rapid development and deployment of services in order to respond promptly to user and CoI needs.

CESs must be readily adaptable in order to satisfy specific requirements of a variety of customers (end users, CoI services). The CESs should be defined independently from specific network and systems technology. Conversely, the exploitation of new technology should be made easier by the flexibility of the service architecture. The CESs should fit in an environment with multiple providers of services. The coexistence of a number of stakeholders, performing various roles, must be supported. In addition, the CESs must provide a flexible framework with respect to changes, and must define an open environment which enables the introduction and modification of services, the introduction and modification of software and hardware components from different vendors and organizations, and the interoperability among such services and components.

A key goal for the CESs is to maximize the use of commercial products and technology, and to focus the limited Government Research and Development (R&D) capacity on unique requirements.

The architecture and engineering of the CESs must enable the management of services and the service infrastructure, and must facilitate the integration of control and management aspects of services. Users must be able to access services independently from the physical location and the types of terminals being used. In addition, the CESs should allow for interworking with existing systems and services, e.g., with Common Operating Environment (COE), legacy, or Web based services.

Benefit of this change in business approach

GES will provide information services necessary for all echelons to better utilize the network for the rapid decision processing necessary to support operations anywhere, anytime, by any user with privileges on the DoD network. GES will change the way warfighters receive and process information. The user will be able to rapidly leverage CoI data producers and their release of real time data to a global data repository for general consumption and decision-making. This availability of information will enable more effective and rapid execution of command and control within a given theater of operations. Other products will include the enabling of technology to allow the access of information by a multitude of appliances such as a dedicated workstation, laptop with a Web Browser, Personal Digital Assistants (PDAs), cell phones, embedded processors, and other computing devices. GES will focus on implementing an open community process, which may include open source, to allow developers the flexibility they need to configure the infrastructure.

Motivation for Changes

In June 2002, during the Joint Military Intelligence College's 40th Anniversary Conference, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C3I) Mr. John Stenbit articulated his vision for information technology as applied to the military in the post-September 11 environment. "DoD must move from an organization with a top-down approach to operations to one that distributes authority for action to 'the edge,'" he said.

Mr. Stenbit called on his audience to move from the centralized thinking and planning currently reflected in the Task, Process, Exploit, Disseminate (TPED) vision to an edge-centered Task, Post, Process, Use (TPPU) approach to information sharing and availability. "We need an environment where users can reach back, that is, pull information they need without having to rely on intelligence production centers to know what users need and push it to them. In this construct, it will be the users, not the producers, who determine what is validated intelligence."

To achieve this change in the culture, in both current thinking and supporting implementations, Mr. Stenbit identified three pillars for change: (1) a ubiquitous network environment, (2) richly populated with information of value, as determined by the consumer, (3) that is highly available, secure and reliable. GIG Enterprise Services will enable the implementation of this, and will also deliver other benefits to DoD:

- **Better End-User Experience** – Data integration adds value. The end-user benefits from the application programmer's ability to efficiently and intelligently combine data from heterogeneous sources. Component models allow services that have been newly written or services encapsulated from legacy applications to be reused. Over time this allows more to be built for less. In the same way, electrical engineers benefit from the use of existing chips and other components.
- **Moving components to infrastructure lowers the cost to the enterprise** – Note that the cost of a service is not just the cost to initially code it. It is also the cost of requirements analysis, design, testing, maintenance and documentation. It has been estimated that most of the true lifecycle cost of a system will occur in the maintenance phase. Therefore being able to re-use a service is a savings at many stages in the development lifecycle. Taking a piece of software off

an "island" and placing it with a defined interface in the DoD infrastructure allows all of DoD to benefit.

- **Enterprise architecture matches organizational goals** – The components in the enterprise should have a correlation to the services offered by organizational elements. For example, the Defense EB Exchange (DEBX) provides an Electronic Data Interchange (EDI) messaging and translation service. This system service correctly corresponds to the functionality defined and offered by DISA APB to the DoD. Considering the components and services in this way allows the architect to conceive of services not yet provided by the infrastructure, or redundant services no longer needed.
- **Closing gaps between "islands of automation"** – This enterprise service approach should provide better efficiencies to the organization by removing the barriers around stovepipe systems.

Service Deployment Models

The GES will be delivered in a variety of forms, tailored to best suit the operational needs of the consumers and the nature of the service being delivered. In general, we can define three basic types of service delivery models that will be employed by GES.

- Policy guidance and standards - This approach will be used for delivery of well-known and stable capabilities that are instantiated as highly distributed capabilities with local deployment. As an example, the Domain Name System (DNS) relies on a strong, stable, specification, with many locally deployed servers supporting the delivery of the service to consumers. For services with similar characteristics, GES will produce and deliver the policies and guidance on topics such as configuration, operations, and deployment, necessary for the service to provide consistency and value to all users.
- Packaged Software - Some services will be delivered by providing common software components, that are used by all providers (or consumers) of a service.
- Networked Service - This will be the goal for many GES; a service operating as part of the GIG. The essence of this approach is that a service provider will be responsible for delivering a service to any qualified consumer within a defined and agreed upon set of parameters. The characteristics of this approach will be discussed in more detail in Section 3.

Design Principles for CESs

The objective for GES is to provide an environment that enables the rapid development and deployment of services, service enhancements and capacity, with agreed upon cost and quality. The services, when implemented should result in well defined, realizable capabilities that can be used within a well-defined architecture with other services to provide a range of simple and complex functions. The following items define principles for designing CESs to achieve the GES goals.

- An open architecture, independent of underlying object models, programming languages, and application platforms. The architecture should focus on allowing systems to communicate in a loosely coupled fashion, allowing any application or system to map its own internal architecture to well defined external interfaces. Use of a layered model, with hierarchy and modularity to support the composition of smaller services in the creation of a larger and more fully functional service. The invocation of one service may lead to the invocation of other services that execute parts of the larger service request.
- Exploit COTS Standards, and Services - Maximize use of current and emerging COTS standards, technologies, products and processes to deliver services and capabilities for DoD

missions. Minimize customization and modification of commercial products and focus R&D and development activity on unique DoD missions and requirements.

- Technology independence - Services should be designed with minimal dependence on specific technologies or vendor proprietary implementations.
- Scale to global proportions - Reduce the tight coupling between service providers and consumers and the requirements for solution specific clients. The need is for flexible and dynamic services that support delivery to thin clients or browser based capabilities, especially those that provide adaptability to a variety of 'edge' environments for end-users.
- End-to-End management - Services must be manageable, both in terms of their own status and performance, and in their interactions with other services. They must provide the means to be created, operated, deployed and destroyed in response to demand and operational needs. The GES CESs must be able to integrate into and enterprise-wide service management capability that enables the near real-time management of business and warfighter processes.
- Accommodate heterogeneity - Services must accommodate different development models, languages, components, etc., and must provide for operations over a wide range of transport services. DoD capabilities will range from low bit-rate tactical communications to multi-gigabit backbone service. End-user devices may range from handhelds and PDA's to laptop personal computers (PCs), workstations, and even mainframes.
- Accommodate continual asynchronous change - The scope of the GES CESs ensure that there will always be changes occurring, as well as changes in the CoI and domain services. It will not be feasible to synchronize them and remain responsive to changing user needs. Modifications to one service must not break the connections to other applications.
- Allow decentralized operations and management - There will be many service providers in the GES environment. Some services will be provided by the military Services, some by the DoD Agencies, and some will be provided by outsourcing to commercial entities. The CES must support federation and interaction among the different parts comprising an end-to-end service offering, and support the integration and operation of warfighting and business processes over the net.
- Provide a full range of performance capabilities, for real time, near real time, and best-effort capabilities. DoD users have varying mission requirements, and will need services that can support a wide range of performance, which may need to be tailored to reflect the availability of transport or computing resources to a user.
- Integrated, layered security - applications require a robust security framework that accommodates the full spectrum of security services including authentication, authorization, integrity, confidentiality, and accountability. The security capabilities must effectively address DoD's complex set of security domains and policies, and also support interaction with the Intelligence Community.

3 Overview Of The Service Model

The DoD, through DISA and other organizations, is planning to be a provider of a set of Core Enterprise Services (CESs) to enable other programs to provide their data and services to the larger community. Increment I is the initial set of CES that the DoD will plan to provide. Increment I covers the time period from approximately 2004 until 2007 and is projected to have several internal development spirals. Other DoD programs will plan to use these core service offerings as part of their move to a net-centric infrastructure.

Core enterprise services (CESs) enable the community of DoD service and data providers on the net.

For many of the participating organizations, the shift from being a developer of system applications to providing "live" operational services on a net will be a significant change in business. Service providers have to construct their offerings in a careful balance between the needs of the consumers, the state of technology, and the cost of providing an operational service. As technology inevitably advances, this balance is constantly reexamined. Service provider quality is often judged on a service's availability, perceived reliability, ease of use, and speed. An active feedback loop that includes consumer impressions of the service provider is vital.

Service Provider Definition

Participants in both the Communities of Interest (CoI) and the enterprise will be offering services in this new net-based model. Consequently, the term "service provider" is used throughout the following discussions. A service provider can be:

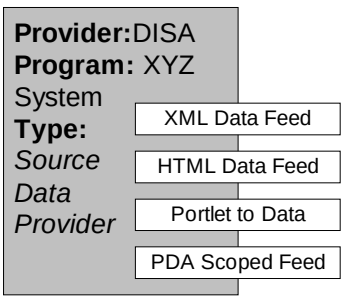
- a source of data to DoD end-users and systems;
- a provider of a value-added service, such as indexing, multiple source data fusion, track management, translation, syndication, or content filtering;
- or a provider of a core enabling service for the enterprise.

For example, a provider of raw data from an Signals Intelligence (SIGINT) feed can be a service provider, while a DoD site that actively indexes that content in a search mechanism also provides a service for the end-user. Another service provider could combine that raw data with other data sources to provide a common fused picture. A service provider can exist within a defined Community of Interest (CoI) or can support the broader DoD community as a core enterprise service. The consumer then has a choice to use a raw data service or leverage the value in a value-added offering.

As the DoD becomes fully net-centric, it is reasonable to expect that there will be thousands of service providers with a wide variety of offerings. As one would expect with a dynamic organization, the ability to innovate will result in service and data offerings that we can not anticipate at this time. When the term *service provider* is used in this document, all the varieties and types of data and value-added service offerings are included.

One System/Multiple Services

What we currently think of as a traditional single system or application can concurrently support many types of services on the network. For example, a data source provider could offer an Extensible Markup Language (XML) data feed from its internal data source and several feeds with user interfaces ranging from HyperText Markup Language (HTML), to portlets, to scoped down Personal Digital Assistant (PDA) data. The final service offerings from a traditional system are a formal or informal negotiation between the service provider and the consumers of the



offering and will change over time. We should not assume that there will be a one-to-one correspondence between current applications and future service offerings.

Platform Agnostic

Service provider interfaces, not platforms, are the issue.

From the consumer's point of view services are "black boxes" on the network, in the sense that their internal implementation is hidden. A service's inputs are specified and its outputs are returned, however, from the consumer's point of view on the outside, the service implementation remains unknown. For example, the platform and database of the service provider are not important to the consumer. This is a divergence from the traditional concept when all program developer's products resided on the same machine. Historically, common platforms were the issue, and the ability to install software on the same machine without interfering with other software was a prime goal. With net-centric service providers, controlled and predictable service interfaces on the net are the issue.

Service Definition

A service may be minimally described by:

- Location on the net (e.g. Address(es) on the Internet Protocol (IP) network) - Service providers on an IP router Wide-Area Network (WAN) will exist at a defined place or places.
- Ports used for communication - The ports that a service provider uses can be a contentious issue. Every port that is used requires the underlying network to accommodate transport of information through that port, and results in modifications to rules in firewalls and other similar devices and changes in network management policy.
- Inputs required by the service - Many service providers require some input parameters before they can perform their service. For example, a Federal Express package location service might require a package identifier to start a search.
- Outputs returned by the service - Many services return information to the consumer. In the notional FedEx example, the location of a package would be returned by the package location service in response to the package identifier.
- Security/access mechanism - Given the DoD context and the networks upon which a service provider will reside, it is likely that a security or access mechanism will be required to utilize most services.

Expanding the definition of a service interface can include items such as:

- Expected response time (during peak and non-peak time periods) - Many performance aspects of a service can be specified, such as its response time. This can be especially important to value-added services who put together information for end-users. Value-added services often rely on the response time of raw data providers in order to present their service within customer expectations. Commercial examples can be seen in the travel reservation industry where multiple data sources are quickly combined to provide a holistic offer to a user.
- Service management method - Service providers must actively monitor and manage the underlying hardware, software, and operational processes to ensure availability and reliability. Service Level Agreements (SLAs) define a contract between the service provider and the service consumer and can define items such as monitoring and measurement mechanisms, performance metrics, compliance, remedies, and termination.

- Cost recovery - In the DoD context most of the services will not require a payment for use, however, this is not unusual in a commercial context. Hosting of applications will involve payment and cost sharing.
- Release scheduling - Service offerings change over time and some method of transitioning between offerings is required.

The Net

At the moment, there is no single "net" for a service provider to live within.

As we discuss the net upon which service providers offer their data and services, we must consider that there is no one net, and indeed currently several logically and physically segregated nets exist within the DoD. The commercial Internet, NIPRnet, SIPRnet, DoD Virtual Private Networks (VPNs), JWICS, and others, are all largely IP-addressable networks that may require separately hosted solutions for core support. For example, offering a security authentication service for service providers on the SIPRnet does not necessarily help providers in the address space of the NIPRnet. Obviously, commonality of core offerings across nets is desirable. Core service solutions, while consistent in architecture across IP-address spaces, will not necessarily be accessible in practice across net boundaries. Multiple hosting of core services will be required, as will interface devices such as gateways and guards that span some of these boundaries.

The core services described in this document are likely to exist in the address space of Operational Area networks (OANs), Metropolitan Area Networks (MANs), and Wide Area Networks (WANs) (both Continental U.S. (CONUS) and Theatres). It is not likely that an *enterprise* service will be created solely for use within a single Local Area Network (LAN) or Campus Area networks (CANs). This is a break from the past, where local LAN-oriented applications were common.

Transition to a Service Provider

The transition of participating organizations into the role of a live service provider on the net is a key challenge. Service providers and their supporting organizations have a number of new concerns including:

- **Managing the configurations of their operational interface** - Service offerings and their interfaces will change over time. Transitioning from today's service offering to tomorrow's more robust offering, will require substantial coordination between the consumer community and the service provider. Since the services are used live on the net, the transition must be time sequenced with all players, even if some parallel operations of the new and old offering occurs. Informing all consumers of a service in sufficient time to allow them to prepare, and possibly test, and modify their applications is a challenge.
- **Publicizing their service offerings** - This must occur with both end-user and technical audiences. Technical staff will need to have the interface specifics that allow them to integrate with the offering. End users will need to understand the value or functionality the offering brings to them.
- **Reaching their consumers regardless of net and infrastructure outages** - End-users will come to rely on the offerings of service providers only when they feel confidence in the high availability of the offering. The net infrastructures that carry service offerings from provider to consumer will continue to have random failures and/or local resource issues at some hopefully low rate. The service provider must engineer their offerings such that a preponderance of the service audience continues to have access to the service during sporadic outages, and in fact, continues to have access during a deliberate attack on the infrastructure. Service providers must redundantly deploy their services to survive net infrastructure failures, deliberate infrastructure attack, and local resource spike or

congestion. Many solutions at the network and application layer are available to mitigate this issue.

- **Gathering consumer feedback and modifying service offerings based on community needs** - Historically, the concept of drawing requirements from the user community has been successfully applied by many DoD applications. The difference in this situation is likely to be the rate of change, the lack of global community build cycles, and dynamic nature of the consumer/producer relationship and its effect on communicating changes in the offering to the community.

Capabilities of the CESs, as described in Section 4, will lower operational risk to the providers of services on the net by addressing the issues above.

Consumers and Producers

Core Enterprise Services (CES) and the Net enable the interaction between consumer and provider.

The net and its supporting CES infrastructure is analogous to a marketplace that allows an interchange between provider and consumer. Figure 3-1 depicts the interaction between service providers and consumers on the net. On the left-hand side of the figure, CoI service providers create service offerings for the net. Service providers can be a source of raw data content being created for the net, or value-added services that perform functions on raw content to make it more useful to consumers. On the right-hand side of the picture CoI consumers make use of the service offerings and feedback in form is given to the service provider. CoI consumers can be end-users, empowered with their ability to directly access a wide variety of content, or value-added services who consume raw data, add value to it, and publish that value-added content back to the net. This entire scenario uses CESs and the net to enable the effective interaction of consumer and producer.

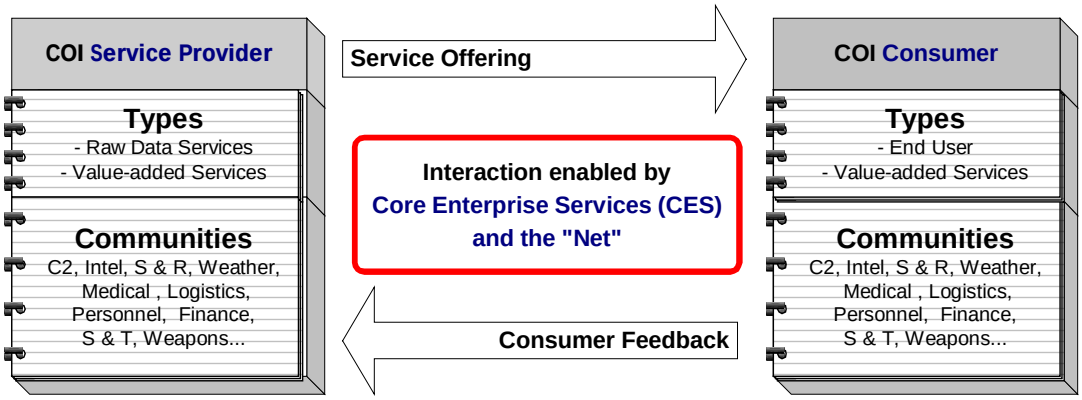


Figure 3-1 Producer/Consumer Interaction

The planned and implemented interaction between a provider and consumer is always a two-way street. Service offerings must meet consumer needs and add value, while consumer expectations must coincide with the state of the art. Consequently, a feedback loop between the consumer and provider should exist not just in the live operation of the service but also in the planning, provisioning, development, and testing of a service before deployment.

Value-added Services

"Increased Specialization and Exchange: Because individuals are endowed with different skills and interests and because the time and resources necessary to learn new skills are scarce, there

is a strong tendency toward specialization in the production of goods and services." Indiana Department Of Education (IDOE 1996)

Specialization is natural consequence of a dynamic marketplace of service providers and consumers. Just like their analogous marketplace counterparts, organizations will tend to leverage their unique knowledge of some part of the DoD domain to produce a service offering on the net. Figure 3-2 depicts the result of specialization where some services provide raw content, and some organize that content in valuable ways for the rest of the community.

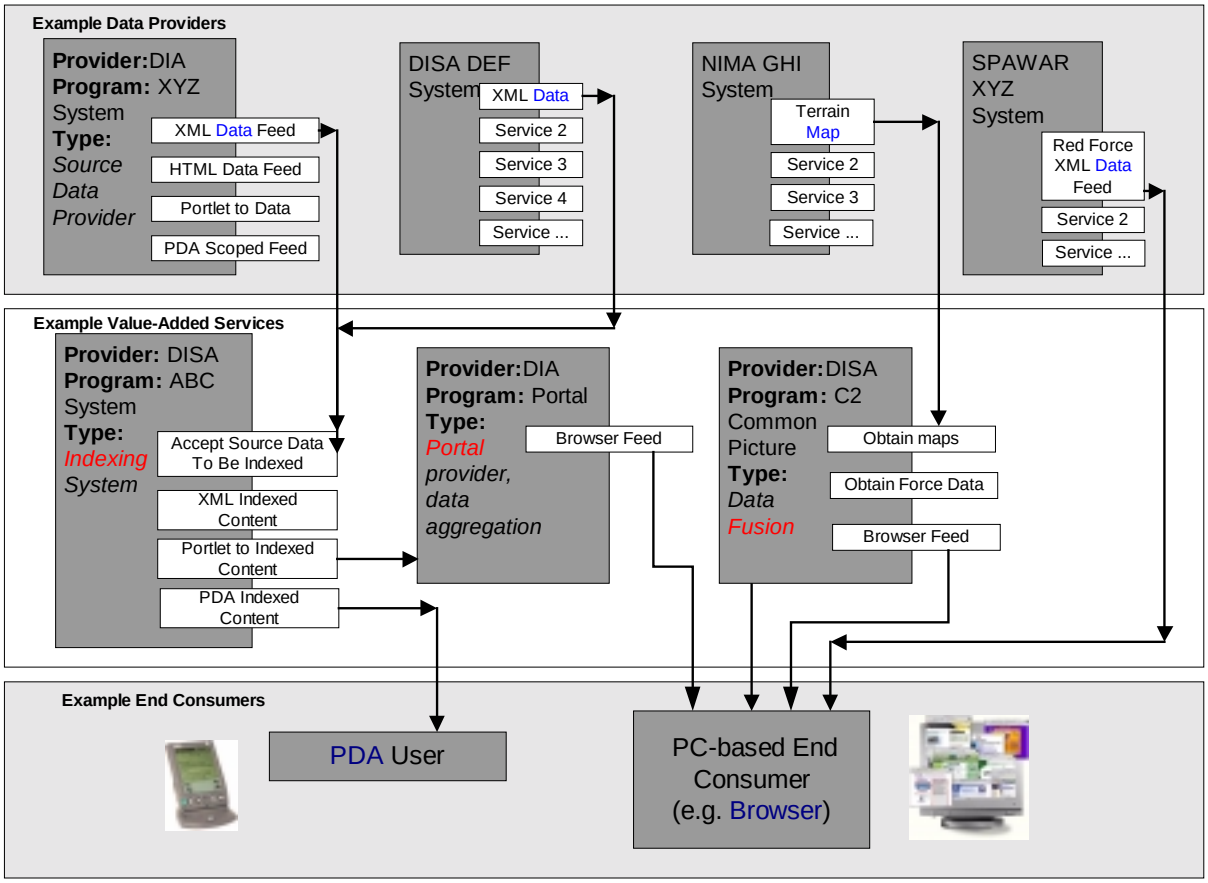


Figure 3-2 Layers of Consumers and Producers

The Task, Post, Process, Use (TPPU) concept that works in conjunction with this layering of service providers is described by OSD as follows:

"To emphasize new concepts of network centric operations and to change common practices of major intelligence organizations, the industrial age concept and acronym "TPED" is replaced with the new concept and acronym "TPPU." Under TPED, collected ISR data is sent to an intelligence organization or element for processing, exploitation and analysis and then disseminated to authorized users. As it has evolved, TPED is inherently a sequential and organization or platform centric approach. This results in a very tight process with little opportunity to open to a wider user set prior to the … dissemination of the processed data … With TPPU, DoD will transform itself to a network centric paradigm of "post before process." TPPU breaks with traditional business practice and allows the ISR community to open its sequential, end-to-end cycle of TPED to allow multiple and simultaneous uses of collected data. TPPU encompasses the traditional functions of TPED yet allows users with multiple information requirements immediate access to collected information. It places those functions in a network centric, information-handling environment.." (OASD(C3I) TPPU Concept for Network Centric Operations 2003)

The Task, Post, Process, Use (TPPU) concept allows end-users in Figure 3-2 to directly access any raw data sources in the domain. However, TPPU does not preclude some organizations from taking raw data sources and adding value to them. Examples of value-added services could include:

- Filtering - For example, selecting a subset of data from an existing raw data stream for a particular classification or audience; e.g. SAR, SCI, GENSER, Unclassified, Coalition partners, etc.
- Translation - Examples: moving data from one set of XML tags to another; moving data from legacy User Defined Formats (UDFs) to XML tagged formats
- Fusion - combining multiple data sources to produce new value-added content, e.g. placing functional area information on a common map
- Indexing - classifying distributed content based on an agreed upon taxonomy to aid search by end-users
- Aggregation - using business rules to combine information in a summarized form

While the figure shows a simplistic three-layer model, there is every reason to conclude that the value-added services would, in some cases, build on one another. For example, a common picture could be built from data that was indexed by another source. In this way the depth of the supply chain can be extended naturally, as long as there is value in it for the consumers.

The CESs are enablers of the raw and value added providers of content and data. For example the CES for Mediation could provide translation, assured delivery, and aggregation tools to the enterprise, and thereby avoid the situation where each CoI must develop a unique or point-to-point solution.

Service Interaction Models

Depending on the type of service, the needs of the consumers, and the nature of the underlying data, there are several generic interaction models for invoking or utilizing services. Usually a service provider will choose one of these models for a particular service offering. The interaction models include:

- **Request/Response** - This is a single interaction usually initiated by the consumer of the service. The consumer creates a logical request for the service and the service answers back with a response. An example might be a lookup or validation service, such as the Fedex service to lookup a package's shipping status.
- **Stream** - In this model a continuous stream of information is created by the service provider. The consumer connects to the stream as needed. Commercial examples include video servers, and financial market indicators.
- **Publish/Subscribe** - Here a consumer registers with the service provider to receive events on a logical device, often referred to as a "channel". Events are published onto the channel, and subscribers receive the events. The events can be complete data objects with fields and attributes. Crossing multiple channels with business rules can allow for high-value events to be generated. For example, events from a "one-way plane ticket" channel could be combined with a "wanted list" channel to produce events of significance.
- **Threads/Process** - A series of sequenced interactions between a service provider and a consumer. Often a set of defined structured messages is used to move the provider and consumer through a business process.

When is a Service in the Core?

While some services clearly, or historically, fall within the purview of particular CoIs or in the core services in general, there are several cases where determining the proper home of a service is not as straightforward. Consequently, it is useful to define the general criteria for capabilities that should be provided by the core set of services. The initial criteria for inclusion in the core services are:

- **The service provides a generic (non-CoI specific) capability to the DoD community**.

  (A service used by one and only one CoI clearly belongs in that CoI.)

- **The service is more operationally effective or cost-effective when procured and/or operated by the enterprise rather than a particular CoI or small group of CoIs**.

  (This refers to issues such as cost, scale, overhead, and licensing. For example, mediation products are effectively licensed at the enterprise level. While many varied products could be licensed one-off at a local CoI level, the cost would be substantially higher. Similarly, the overhead costs of help desks are best distributed across the support of multiple services.)

- **The service supports, or is capable of inherently supporting, more than one CoI.**

  (Note that the consumers of a service are a dynamically changing group. A useful service may be used by two CoIs today, and many more tomorrow, depending on marketing awareness, and program transition schedules. New services, even core services, will take time to reach enterprise marketshare, and they should not be penalized too early in their growth. This is ultimately a judgement call of the Steering Group.)

- **The service provides a mandatory function or capability in the GES enterprise architecture**.

  (For example, it is possible to allow every service provider to design and build their own security and management schemes. Having hundreds or thousands of security and service management solutions would severely hamper the rapid and dynamic use of services by consumers. An architecture that defines participation in the offering of net-based services will specify the rules of engagement for service providers. The architecture will make use of some offerings, or range of offerings, mandatory. For example, there could be a set of approved security mechanisms for service providers.)

The following section defines strategies for the individual CESs, and capabilities attributed to the CESs over time, that are in consonance with the criteria described above. A capability can be considered a candidate for a core service by meeting one or more of the criteria above.

Lifecycle of a Service: An Activity Model

In order to aid the interaction between consumer and provider, services must follow a predictable and structured life-cycle from their initial creation to their final retirement. Figure 3-3 depicts an activity model for the life-cycle of a service.

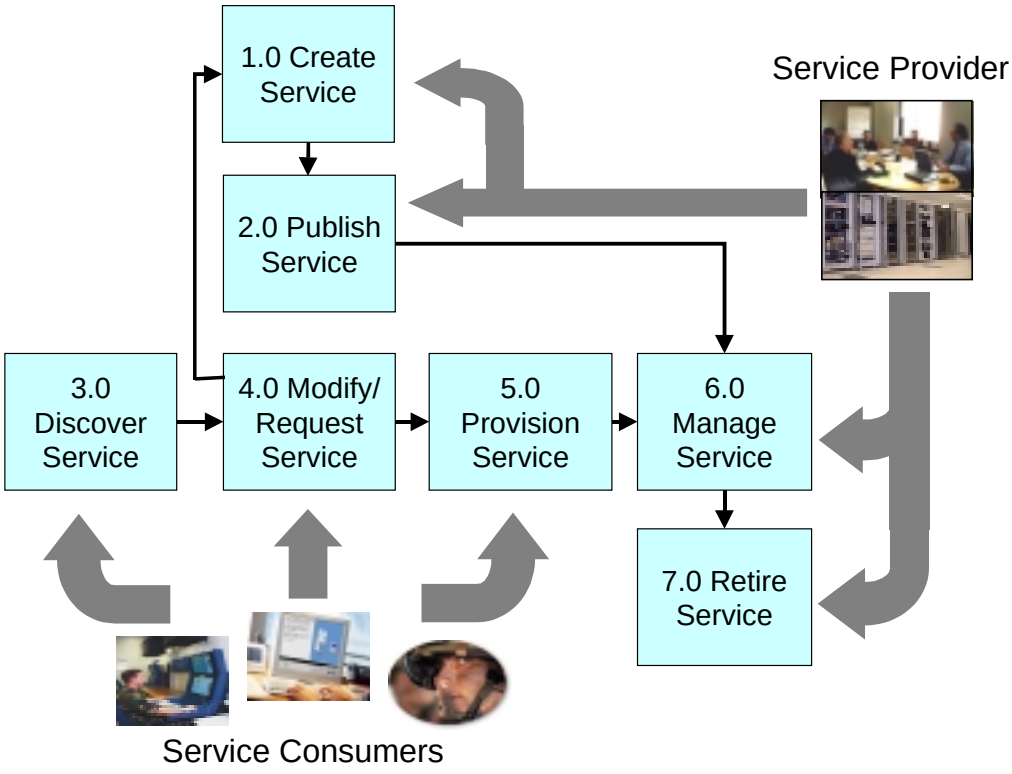


Figure 3-3 Service Offering Life-Cycle

Table 3-1 describes the notional steps in a service offering's life-cycle as depicted in the previous figure.

Table 3-1 Service Offering Life-Cycle Steps

Lifecycle Step	Step Description
Create Service	Services are created to solve market or community needs. There are a number of steps in creating a service, which are beyond the level of discussion for this figure. These steps might include activities like requirements analysis, coding, several types of testing, and fielding. We will assume that a structured engineering process is being used to create service offerings for the community.
Publish Service	After service providers have created a potential enterprise service it must be offered to the community through a publishing mechanism. Publishing a service begins with a registration process. The registration capability allows a system's Program Manager (PM) or Executive Agent (EA), generically called a service provider, to define the services of a system within a registry. During the registration process a service provider will use the registry GUI to define the various aspects of the service being registered. A registry will act as a persistent store for the attributes and objects that describe a service. The service provider will provide information to the registry about the service including: • Points of contact for the managers organization • An Interface Specification (IS) for the interface • Service metadata about the interface • Optional legal information about the interface • Optional Quality of Service (QoS) data about the interface Optional security specifications about the interface

Lifecycle Step	Step Description
Discovery - Finding a Service Offering	One of the most important aspects of a service-oriented architecture is the discovery of services. The discovery of services is done for the purpose of end-user consumption and business-to-business (B2B) service integration. The search to discover services may be driven through a number of methods, including pre-sorted lists, category searches and/or free text searches of descriptive fields. Initially, the discovery registry will support design-time integration of service offerings. This means that technical staff will use the GUI provided by the discovery tool to seek out and discover needed services, and that they will then alter their application systems to access or invoke the discovered systems. This process retains human decision points and human control throughout the integration.
Modify / Request Services	If an applicable service has not been found, a consumer can suggest a modification to a service, or post a request for a service that service providers can view and optionally address. To modify a service offering the user must first find an existing service that will support modification. The consumer can find a service that seems close to the consumer's needs and a modified form of the service can be proposed back to the service provider. Using collaborative capabilities, the consumer and provider may be able to create an arrangement that leads to a new service that others may also use.
Provisioning Services	After a service has been discovered, the service consumers must decide if the service meets their needs. Aspects of the service under consideration include attributes such as; expected Quality of Service (QoS), terms-of-use, period-of-service, potential legal agreements, and technologies used in the interface. If the service meets the needs of the service consumer, a decision to provision the service is made. The provisioning process may be specific to the providing organization, and could span the range of interaction from simple click-and-download, to extensive human interaction and contractual agreement, although maximum automation is encouraged. The provision process ends with the access to an service interface specification (IS).
Management of Services	Once services are available on the net, they must be managed to maintain the consumer's expected service performance levels. The management of the service is directly related to the expected role of mediation in the use of the service and the use of Enterprise Service Management (ESM) capabilities.
Retire Services	When a service is shutdown or retired and is no longer operational, then the registry and its service offering metadata will be updated. Services may be retired for any number of reasons, and thus the overall architecture must accommodate this. The service provider must review the commitment to the current service consumers. If there are ongoing consumer commitments, then the service provider should contact the consumers to negotiate an amicable solution. If there are no such commitments, then the provider may end the service after informing the consumers in the form of a service retirement or transition plan. In either case, the publishing of the plan should be followed by some period of time set in the blanket agreement for publishing a service. In the case of a transition, the transition service should be running and tested by the transition service consumers before the original service is retired.

Compliance Considerations

There are a handful of structured steps that a service provider should go through before being universally available to a community on the net. These process steps insure that the provider will be highly available, survivable, and effective in offering a service to community consumers. Formalizing these steps lowers the performance risk for service providers and increases the likelihood of service acceptance by consumers. (It is not the intent of this section to specify a compliance policy, but rather to bring up the issues that should be eventually considered.)

Before the compliance process begins, we can assume that certain key technical program management documentation will be in place. In particular, two key documents are required before the Communities of Interest (COIs) can effectively develop service offerings to share with the enterprise community. These documents include:

- **Architecture documents** - describes the Core Enterprise Services (CESs) in terms of an As-Is and a To-Be vision. Defines a transition plan to get from the current architecture to the next milestone in the future. (The architecture documents will contain some form of the required C4ISR figures though we recognize that these may require enhancements for representing one-to-any Service Oriented Architectures (SOAs).) The architecture aids the service provider developer in knowing how to understand the architecture of the services today and *where the CESs are moving strategically over time*.
- **Developer's Guide/Specifications** - describes the process of creating and fielding a compliant service. This document completely defines the current technical methods for connecting to, utilizing and/or integrating with the existing core services. The specifications define the technical interfaces to the underlying services.

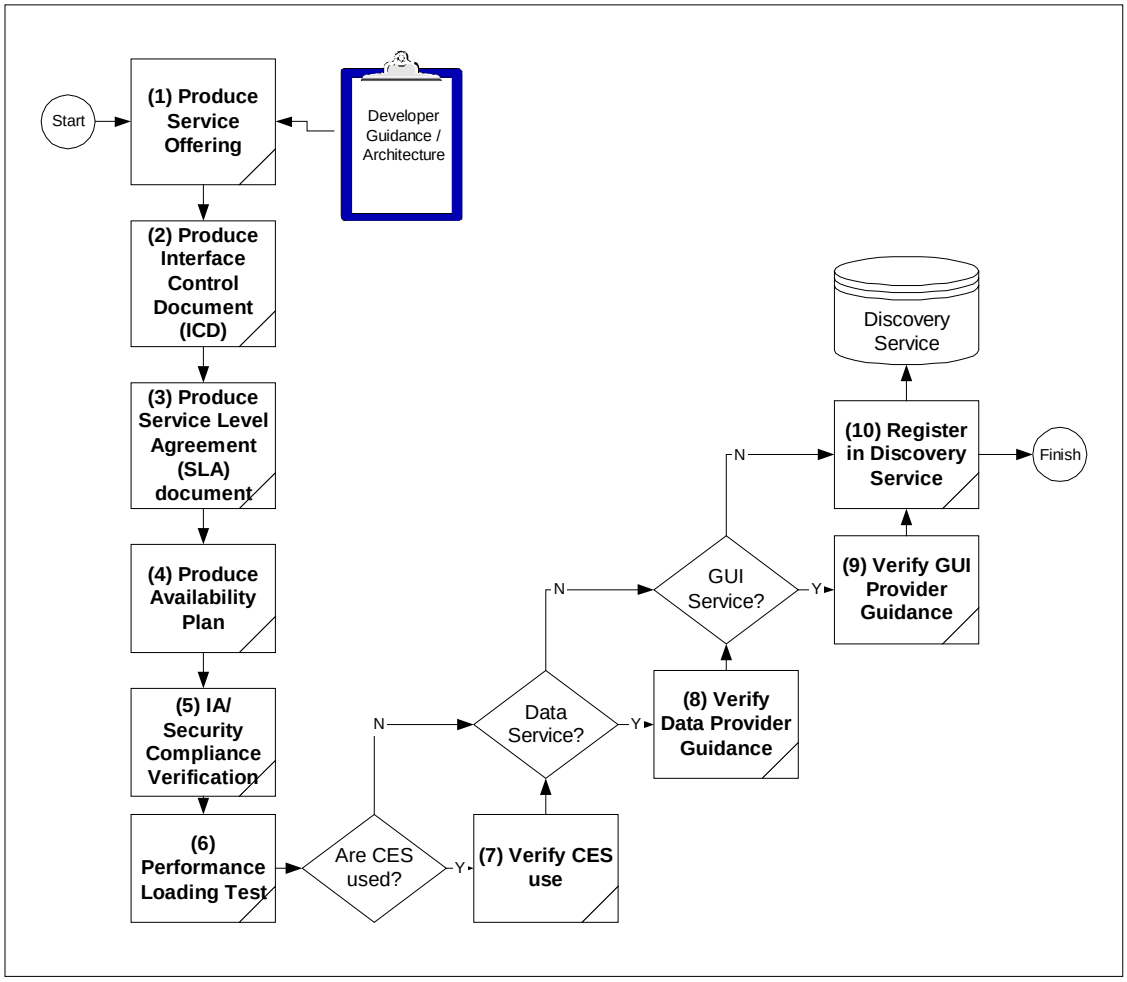


Figure 3-4 Notional Compliance Process for a Service Offering

Figure 3-4 depicts a notional compliance process at the highest level. The figure depicts the nominal flow through the compliance process, and does not show compliance failure loop-backs at each step for clarity. Table 3-2 describes each of the possible steps in the process in more detail. This discussion is only notional and is not meant to convey a new policy or guidance.

Table 3-2 Notional Compliance Steps

Step	Description
(1) Produce service offering	In this step a providing organization recognizes a need/requirement on the net for a particular service. The organization, which hopes to be a service provider, creates the service, either perhaps from a legacy system or as an entirely new offering. The organization performs the engineering needed to determine: •Which net(s) the service offering resides on (e.g. SIPRnet) •Where the audience for the service is in terms of the net topology (e.g. in theatre, or mostly CONUS) •Approach for service availability, survivability, (e.g. specify redundancy, fail-over, load-balancing etc.) •Operational support for the 24x7x365 service Finally, a potential service offering is created.
(2) Produce Interface Control Document (ICD)	The ICD describes the interface of the service offering on the net. The document will describe: •Location(s) of the service •Expected interaction with the service by consumers •Technical specifications for using the service The document can be supplemented with a WSDL description of the service, if applicable.
(3) Produce Service Level Agreement (SLA) document	This document is an offer from the provider. The SLA becomes an agreement, between the service provider and consumer. The document will describe: •The promised response time of the service •Fee for service use if applicable •The eventual retirement mechanism of the service and the transition mechanism to a new service •Remedies if the service does not perform as expected •Termination
(4) Produce Availability, Survivability Performance Plan (ASPP)	As good engineering organizations, this work should have been performed already in the development of the service. This document formalizes the decisions made by the service provider. The document describes the service providers approach to: •Redundancy •Fail-over •Load-balancing
(5) IA/Security Compliance Verification	This step produces a measure of the use of the CES for IA/Security. When the IA/Security CES is fully defined, there will be a mechanism to determine if the participating service providers have complied with that implementation. The enterprise does not want each service provider defining a new security mechanism.
(6) Performance load testing	In this step the service is made operational in some realistic IP-WAN testing environment. The expected load for the service is artificially generated and the performance of the service offering is measured. The expected load will be based in part on factors defined in the ASPP document such as the projected audience and hosting redundancy.

Step	Description
(7) Verify CES use	There are several compliance steps that do not apply to every service provider. For example, not every service provider needs the capabilities provided by each of the Core Enterprise Services (CES). If the CES are not needed, then there is no need to test for compliance with them. However, a Community of Interest (COI) application should not re-invent, re-purchase, or field a service that is already covered by the CES. This step will be more definitive when the technical mechanisms that implement the CESs are known.
(8) Verify data provider guidance	A service may be a fundamental provider of data into the net. If a service offering is a data provider, then the data should ideally follow the following rules: • The data should be exchanged in an XML format. (How it is stored internally is not the business of the consumer.) • The data should use an XML schema registered, or effectively in the process of being registered, in the XML Registry
(9) Verify GUI guidance	A service may be fundamentally structured for end-user consumption in the form of a Graphical User Interface (GUI). Examples of GUI services could include portlets, HTML, allowable scripting languages etc. If a service is a GUI provider then the appropriate GUI guidance documents should apply. These might include: • Complying with section 508 guidance • Complying with portlet guidance when appropriate • Complying with HTML guidance when appropriate
(10) Register in the Discovery service	Having successfully completed the previous steps, the service provider is now ready to register the service with the Discovery CES tools. This implies that the offering is now *operational* and has complied with all the previous steps as appropriate. Service offering that do not comply with the previous steps should not be allowed to register in the Discovery CES for broad community access. The service provider will register on the Discovery tool appropriate for the net(s) where the service will be available.

1

4 Strategy for the Core Enterprise Services

The following sections define each of the Core Enterprise Services (CESs) and describe a strategy for Increment I and beyond.

4.1 Enterprise Service Management

ESM - Basic Capabilities

- Infrastructure/service management
- Cross-domain management information exchange
- Cross-domain IT situational awareness and mission impact assessment
- High service availability assurance
- Supporting policies and procedures

In a net-centric environment the increasing dependence on distributed mission critical services and net-based capabilities makes the end-to-end operational management of the underlying infrastructure a mission-essential task. To support mission critical services, the underlying infrastructure must be planned, built, sized, implemented, operated and managed to meet target, end-state GIG operational requirements. Further, ESM solutions for non-deployed and deployed environments must be: capable of supporting 24x7x365 operations; at least as reliable as the systems they support; meet current and emerging security requirements; be interoperable across traditional organizational management and security enclave boundaries; and be easy to use and maintain with effective service desk support.

Within GIG Enterprise Services (GES), the term Enterprise Service Management/NetOps (ESM/NetOps) describes the critical enabling service that will allow GES to implement NetOps concepts that will provide assured end-to-end service availability, assured Information protection and assured information delivery. The inclusion of NetOps as an integral part of the ESM service is indicative of the importance that sound operational concepts will play in the successful implementation and operation of the GIG.

The ESM/NetOps service will provide the suite of operational processes, procedures and technical capabilities needed to ensure that GIG Enterprise Services (GES) are up and running, accessible and available to users, protected and secure, and that they are operating and performing within agreed upon parameters. ESM/NetOps also ensures that problems are proactively detected, isolated and resolved with the minimum impact to the user. ESM/NetOps consists of capabilities and activities like: fault, configuration, accounting, performance and security management (FCAPS) of all GES components; service and help desk support (e.g. 911/411, user support, problem reporting, etc.); service planning and provisioning; service level management; and IT event correlation and mission impact assessment.

ESM/NetOps will initially focus on the GES portion of the GIG. However, since NetOps is a broader DoD-wide concept, it is anticipated that many of the ESM/NetOps policies and operational processes and procedures supporting the development and implementation of GESs will be directly applicable to the entire GIG.

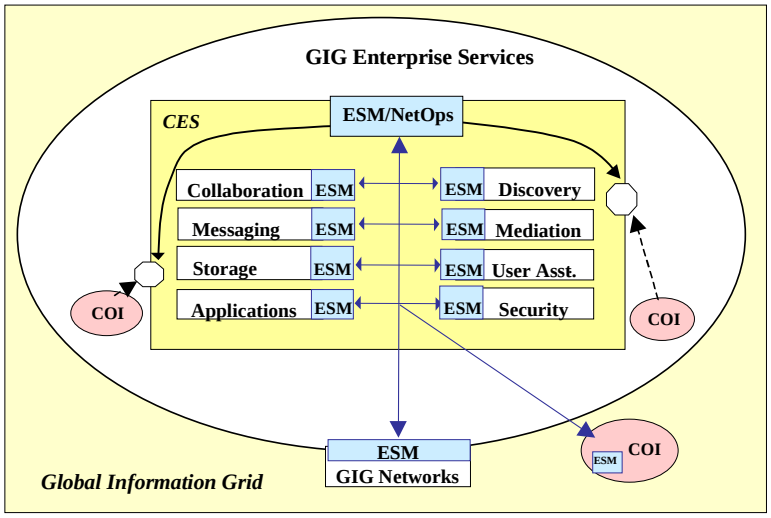


Figure 4.1-1 ESM/NetOps Service Scope

GESs represent shared critical Information Technology (IT) services that together will form the underlying foundation of the GIG. As such, they must be actively monitored, controlled and managed. ESM/NetOps will be the operational management solution employed by all CES and CoI services participating in the GES shared space. It will also be the service that is used to monitor, control and manage all CES and CoI services in the GES shared space to ensure and enforce compliance with GES ESM/NetOps policies. As shown in Figure 4.1-1 above, this means that ESM/NetOps will be an integral set of capabilities that must be built-into every CES and CoI service as well as being a stand-alone service or functional capability that will be used by prospective service providers to proactively management critical GES components.

4.1.1 Strategy For Increment I

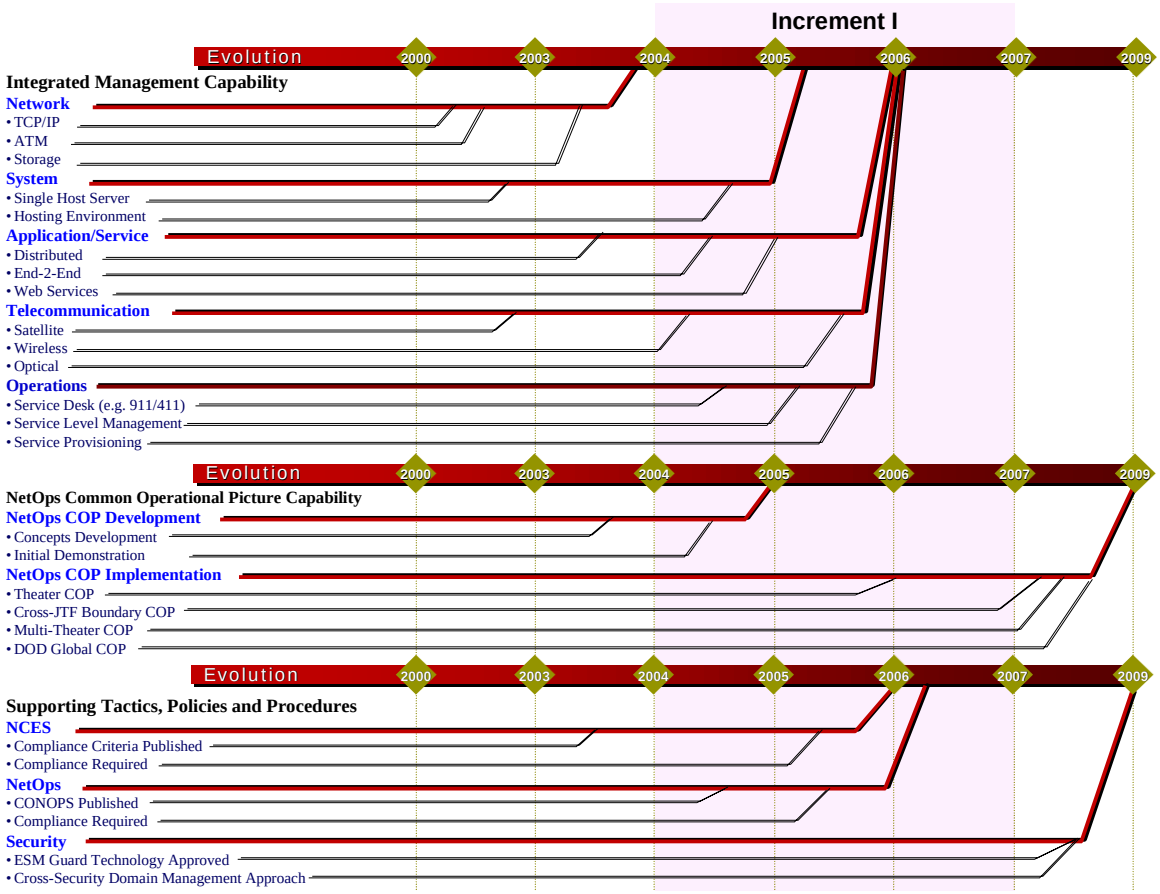


Figure 4.1.1-1 Enterprise Service Management–NetOps Evolution

Integrated Management Capability

Integral to achieving and maintaining information superiority will be the ability to actively monitor, control, and manage DoD's worldwide infrastructure so that it directly supports the accomplishment of the mission. In many respects this ESM-NetOps approach represents a major departure from the current situation where IT is managed on an enclave or domain basis with little or no exchange of management information taking place between management facilities in that it *mandates* an increased level of information sharing and integration between management operations across different technology, operational, and security domains. This increased level of cross-domain coordination and integration is essential to achieving and maintaining information superiority.

This is not to say that ESM/NetOps is intended to be a way of integrating or migrating all of the existing management solutions into a single solution, e.g. IP, optical, terrestrial communications links, satellite communications systems, voice switches, etc. rather it is recognition and acknowledgement that there must be significantly increased levels of meaningful management information exchanges among the organizations, facilities, and operational managers responsible for managing the GIG.

Current operational DOD IT infrastructure management technologies and operational processes are firmly rooted in the management of the underlying telecommunications systems and the core elements of its TCP/IP networks, e.g. NIPRNet, SIPRNet and JWICS. While logical given the way in which communications systems and networks have been developed and deployed and almost universal in implementation, the well understood and documented management of telecommunications and network devices by itself does not begin to address the requirements of managing the total GIG infrastructure.

The concepts, technical solutions, and operational processes that have given today's GIG networks the status of being utilities, in that they are universally available and dependable, must now be applied to other elements of the GIG infrastructure such as services, systems, and functional applications. While systems, e.g. computing platforms and operating systems, are currently being managed, they are not being managed as consistently as network devices and sharing information about the status of a system or application is not nearly as common or as standardized as the sharing of similar information about network devices. This is especially true for systems or applications that, while logically integrated, may in fact be geographically distributed around the world. Application management, especially in a widely distributed computing environment, is neither well understood nor is it widely implemented and while everyone generally agrees that better management of systems and applications is necessary, there is little agreement on exactly what that means or how it should be implemented.

A key underlying tenet of ESM/NetOps is that all CES and CoI services must be "manageable" in all deployed operational environments. This means that they must be equipped or instrumented with the appropriate set of built-in functional management capabilities and that they must support agreed upon operational policies, processes and procedures. For GES Increment I this means that every CES and CoI service must be able to securely monitor and detect changes in:

- The activity of critical processes and resource utilization and accurately and securely report anomalous behavior that breaches agreed upon thresholds
- Their operational configuration and accurately and securely report any changes in configuration or operational status
- Their overall operational performance and accurately and securely report any failure to meet agreed upon service level agreements
- Their security status and to accurately and securely report on any changes in security status to include any anomalous security behavior that could be indicative of a cyber-attack directed against the service

In addition, all deployed services must:

- Meet minimum DoD IA requirements as outlined in DoDD 8500.1 *Information Assurance* and DoDI 8500.2 *Information Assurance Implementation*
- Provide adequate and timely service desk support and
- Support ESM/NetOps trouble identification, reporting, escalation, resolution and notification processes and procedures

To facilitate consistent development and implementation, the ESM/NetOps service will develop guidelines for other CES and CoI services to follow in developing and implementing their operational

management capabilities as well as compliance criteria that will be used to ensure that management capabilities are correctly implemented and that they support approved operational policies, processes, and procedures.

Along with the need for secure monitoring and reporting capabilities described above, ESM/NetOps will address additional security requirements. Since its' inception, Network and Systems Management (NSM) has included security as a key component of the "FCAPS" however it was not until the widespread implementation of DoD's Defense-In-Depth approach to Information Assurance (IA) that IT security received much attention. Under emerging Joint doctrine, IA is now an integral part of NetOps and as such it will be an integral part of the GES ESM/NetOps service to include monitoring, managing, and controlling the operation and performance of IA components like firewalls and Intrusion Detection Systems (IDS). ESM/NetOps does not however include other security activities like certification and accreditation under the Defense Information Technology Security and Accreditation Program (DITSCAP).

NetOps Common Operational Picture Capability

Given the increasing complexity of the distributed DoD computing environment and underlying IT network infrastructure, the root cause of a particular problem may not be readily apparent. As the type, number, and complexity of the systems overlaying the GIG continues to grow, individual management teams will be increasing unable to determine the specific cause of a problem or even to assist a user in making their initial trouble report. ESM/NetOps represents a fundamentally different way of looking at an organization's IT infrastructure where multiple teams work together, forming operational relationships that cut across traditional organizational, management, and domains.

> *"Due to the nature in which the GIG has evolved, the Department of Defense's global communication networks are currently managed and controlled as a loose confederation of networks with no central authority, oversight or guidance. This transformational Information Superiority capability envisioned in Joint Vision 2020 (JV 2020). This will require the ability to collect, process, disseminate and exploit an uninterrupted flow of information while denying an adversary's ability to do the same. To achieve such a dominant advantage, the GIG requires end-to-end management, control and optimization, providing assured service to senior leaders, commanders and warfighters at all levels. This, in turn, depends upon achieving and maintaining near real-time situational awareness of GIG resources." (MCEB 2002)*

Current operational management implementations are typically restricted to a single management domain or to a small number of organizationally or geographically related domains. Sharing between different domains is normally hampered by any number of factors including but not limited to differences in culture, policies and procedures, and management products that are employed. Some of the most commonly encountered problems include:

- Operational managers from different management domains many times do not share a common understanding of what an "event" means, therefore it is easy for them to look at the same data (each from their own unique perspective) and draw different and sometimes wrong conclusions.
- Lacking a common operational understanding, network and systems managers sometimes feel that they must independently assess the potential impacts of a network event on their particular system since the "other" team may have misinterpreted the data.
- Without a common operational network picture and body of management policies and procedures, two management teams may each think that the other is working to resolve a problem when in fact nobody is working on it.

These kinds of situations are far too common and result in significant amounts of time being spent diagnosing the wrong fault resulting in increased down time, multiple managers trying to manage the same object resulting in duplication of effort, a lack of continuity in problem resolution operations, and a generally decreased overall efficiency in IT management operations.

NetOps is the coordinated and comprehensive set of operational concepts and organizational structure that will "fuse" Systems and Network Management (S&NM), Information Assurance/Computer Network Defense (IA/CND) and Information Dissemination Management (IDM) into a single integrated operational construct. This fusion of what are currently three separate disciplines will provide the Warfighter with the policies, processes, procedures, tactics and tools needed to actively monitor, control and manage the GIG. NetOps concepts are based on a combination of organizational, procedural, and technological activities focused on: (DoD CIO 2000)

- Linking widely dispersed network operations centers together through command and organizational relationships
- Establishing joint tactics, techniques and procedures
- Establishing a technical framework that will enable the creation of a common network picture

Creating an cross-domain IT situational awareness capability or common operational picture requires an infrastructure that has been instrumented with monitoring and reporting capabilities, an in-depth knowledge regarding critical mission processes, an understanding of the relationships between the two, and the ability to present relevant status and associated mission impact assessments to decision makers at all levels.

When coupled with the right technology, ESM/NetOps concepts will enable organizations to build a consistent "view or picture" of the status of networks, systems, applications and their inter-relationships that make up their portion of the GIG which can then be shared with other management teams to form aggregate views. This kind of managed information sharing is critical to end-to-end performance monitoring, analysis and optimization and to IT event correlation and mission impact assessment. These two capabilities represent the longer-term goals for Increment I of the ESM/NetOps service and their realization will require significant changes in current operational polices and implementations as well as advances in management and security technologies.

Supporting Tactics, Policies and Procedures

The kind of multi-domain federated operational environment envisioned by ESM/NetOps represents a fundamental shift in managing the GIG. Current network and systems management implementations are typically restricted to a single management domain or to a small number of organizationally or geographically related domains or enclaves. Sharing information between management domains under the operational control of different management facilities is typically hampered by any number of factors including but not limited to differences in culture, policies and procedures, and management products that are employed. While most of the Services and Agencies have developed and implemented extensive policies and procedures for use within the domain, there are currently no clear cut policies and procedures in place for cross-domain management information exchanges and although extensive sharing of management information does take place, it is typically on an ad hoc pair-wise basis.

The ESM/NetOps service will develop the necessary set of cross-domain operational policies, processes, and procedures, based on internationally accepted common bodies of knowledge like the Information Technology Infrastructure Library (ITIL) and the TeleManagement Forum's Telecommunication Operations Map (TOM), needed to enhance the flow of information between different management domains thereby allowing for the quicker and proactive resolution of problems and improved planning and provisioning through better communications of requirements. This will also provide the foundation

for implementing a DOD-wide IT Service Level Management capability to ensure that more consistent levels of service are provided to the Warfighter.

4.1.2 Strategy Beyond Increment I

ESM/NetOps is absolutely critical to the operational success of GESs and the GIG. It will bring the critical policy and technical mechanisms needed to ensure the security, availability and operational readiness of the GESs. This means that the majority of all required ESM/NetOps capabilities must be front-loaded and developed and implemented as quickly as possible by every other CES and CoI service. Given the magnitude of the operational changes to existing operational policies, processes and procedures posed by NetOps, it would not be unreasonable to expect that fully implementing them across DoD will extend into Increment II.

Enhancements beyond Increment I will primarily involve technology refresh and the development and integration of management capabilities for any new technologies as may become widely available. In addition, it is anticipated that advances in technology during this timeframe will also enable DoD to implement networks, systems and applications that exhibit significantly improved fault tolerance and that are to some degree both self-diagnosing and self-healing.

4.2 Messaging

Messaging - Basic Capabilities

- Browser-based email
- Instant Messaging
- Lightweight wireless support
- Unified fax, paging, voice, and video service
- Interoperable global communications

Messaging is one of the Core Enterprise Services (CESs) within the Global Information Grid (GIG) Enterprise Services (GES) that compliments other services such as Collaboration, Mediation and Discovery to provide a comprehensive access to information anytime and anywhere. Traditional messaging involves multiple participants relying mostly on stationary infrastructure and communicating with each other using richly featured devices that are relatively static. Application of security requirements on top of traditional messaging, while vital, further restrict the range and flexibility of communications and access to information. Messaging within GES will overcome these limitations by allowing a wide range of devices from fully featured to thin clients to operate in static as well as mobile environments. Requisite level of security will be met by several mechanisms, both hardware (e.g. the Common Access Card) and software (e.g. Class 4 DoD Public Key Infrastructure (PKI), currently under development). These mechanisms will be implemented at both the client and server levels. Security capabilities related to Messaging for users/applications/devices will depend on Information Assurance/Security Services as described in Section 4.8.

The primary mechanism that can span a wide range of devices is that of Web-based Messaging taking advantage of HyperText Markup Language (HTML) and eXtensible Markup Language (XML). This browser-based access will facilitate integration with other GES services as well as dovetail comfortably with Combatant Commands, Services and Agencies (CC/S/A) thrust into Web portals. The client browsers could span the range from high-powered desktop computers to thinly featured cell-phones and other short messaging devices. Another area where GES Messaging will distinguish itself from traditional messaging will be that of Unified Messaging that will allow E-Mail, Fax, Paging, Voice Mail and Video to be accessed from a common device. Other Messaging services will include presence detection and secure instant messaging regardless of the location and connection method of the participants. Notification to selected devices will be made using the publish and subscribe *push* and the publish and subscribe *pull* technologies

Messaging Services Components.

GES Messaging can benefit from the previous studies and initiatives that were performed to further messaging technology and services. These efforts recommended moving away from the current End-to-End messaging architecture for scalability, maintenance and cost reasons. Three other alternatives included the Boundary-to-Boundary and Centralized Staging Server, and Hybrid messaging architectures. These may also be implemented through a centralized message store within a Unified messaging architecture. These efforts will be integral to providing a logical roadmap to a Unified Communications and Video Real Time Enterprise (RTE). The various components that make up the Messaging Services and the estimated time frame during which they may be achieved are shown in Figure 4.2.1-1: “CES – Messaging Evolution”

4.2.1 Strategy For Increment I

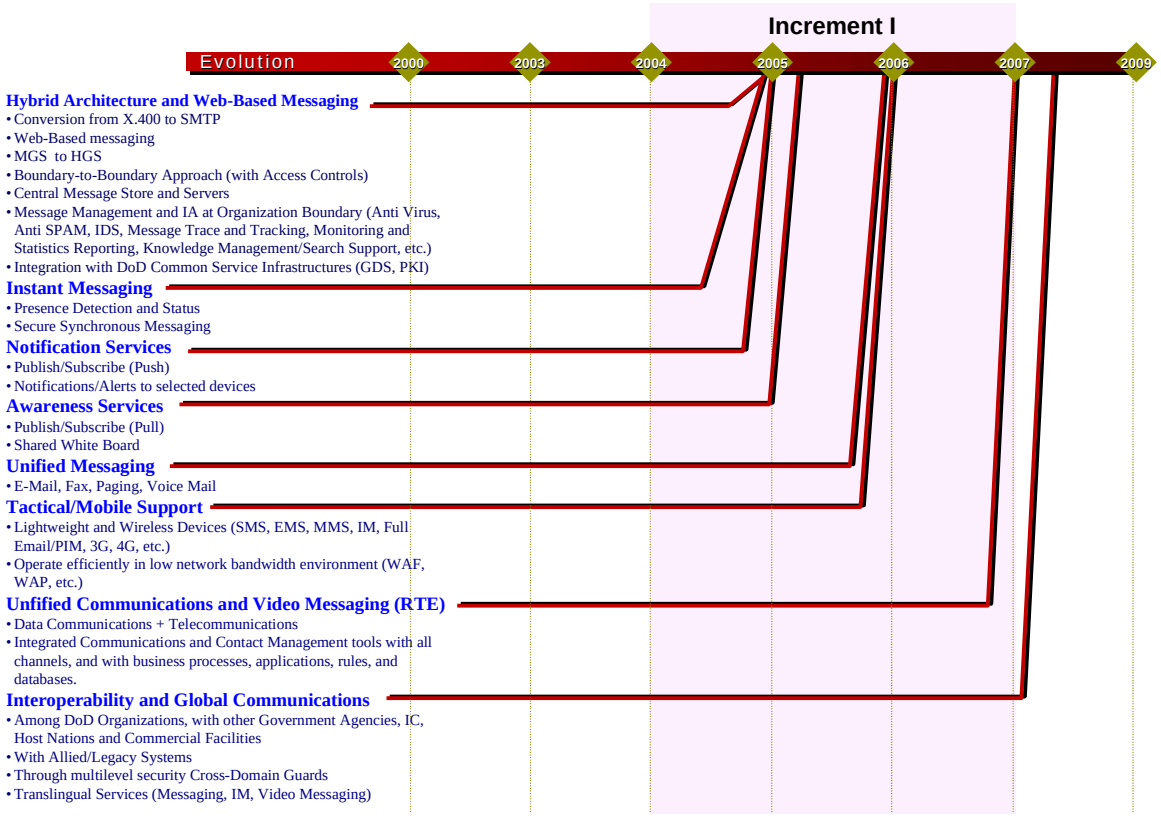


Figure 4.2.1-1 Messaging Evolution

Hybrid Architecture and Web-Based Messaging

Although high assurance is one of the primary factors, GES Messaging can start with the available Commercial Technology Baseline within legacy programs and initiatives (i.e., Medium Grade Services (MGS) based on Simple Mail Transfer Protocol (SMTP)) and then add in the DoD High Grade Services (HGS) capabilities. The Web Browser is the preferred user interface because of its versatility and widespread use and availability from desktop to cell phone and PDA. Another impetus to Web-Based Messaging comes from Combatant Commands, Services and Agencies (CC/S/A) who are implementing various portal-based services for their individual organizations. Commercial products are also moving toward web-based messaging for achieving equivalent level of security as offered by on-line transactions such as banking and e-commerce. Web-Based Messaging can be implemented in either the Boundary-to-Boundary or Centralized Server architectures. The architecture will rely on the integration of Messaging with DoD Common Service Infrastructures such as Global Directory Service (GDS) and PKI. Messaging Services will rely on the Information Assurance/Security Services for providing access control, authentication, confidentiality, integrity, and non-repudiation for the users/applications/devices. Message Management and Information Assurance will be established at the organization boundary.

Instant Messaging

Instant Messaging (IM) is one current form of synchronous messaging. The use of IM is increasing at an astounding rate in both consumer and business applications. Primarily, IM is being used to replace phone calls, short, basic e-mail, and organizational messaging when immediate responses are needed. It is purely interpersonal; applications use mediation technologies, which have error checking. Infrastructure is in place for rapid growth in the future. Secure IM could be an excellent method to push

out flash traffic, and high-precedence messages needing immediate action by users. Before secure IM can be implemented, presence tracking across multiple organizations and in various environments and robust archival/retrieval mechanisms would have to be achieved.

Publish/Subscribe: Notifications Services (Push) and Awareness Services (Pull)

Notification Services will send notifications to subscribers using the subscriber's choice of notification medium (e-mail, telephone, pager, fax, wireless) with an option to request a response. Commercial implementations include: airline flight schedule changes, stock price changes, auction bid action, etc. Recipients with access to a Web browser can contact the Web site to respond. Subscribers can tailor their preference by time of day.

Awareness Service has been around for a long time. There are several groupware products (i.e., NNTP, etc.) that provide this type of functionality. Essentially, messages are posted to an electronic "board" kept on the server and then users with access to the "board" can retrieve the messages. The messages can be kept on the server for a configurable time and can also be stored locally. Awareness is used here in a limited sense; for a broader concept of Awareness refers to Mediation and Discovery Services.

Unified Messaging

Figure 4.2.1-1 Notional Unified Message Store

Unified Messaging is becoming prominent, as it helps to merge the user's voicemail, e-mail, pager and fax messages into a single queue of tasks to be handled, and makes them available from telephony, desktop, kiosk, fax or mobile devices. In the user's familiar email inbox, a unique icon identifies each message type. Unified Messaging provides the professionals with more flexibility when traveling, improve user productivity while in the office or on the road. Vendors and Enterprises, however, should remember that ***Unified messaging is only one step along the path toward a broader Unified***

Communications service offering. Most industry experts believe Unified Messaging will have a life cycle of five years at best.

Tactical/Mobile Support

Tactical/Mobile users need wearable, light-weight wireless devices that can endure and withstand rough weather and mobile environments. Wireless is evolving quickly; 128-bit SSL to a hand-held microbrowser is available today. Once there are unique identifiers on devices, encryption/decryption capability on the handheld devices, fingerprint readers on Palm devices, etc, then there will be more and better options for protection of information. All these enhancements are expected to arrive this coming year (2004).

Messaging vendors have unique features for tactical/mobile users need to operate efficiently in low network bandwidth environment. Some of the main features include mailbox caching, data compression, slow-network detection and conditional up/down operation, quick setup, configuration and jumpstart, distributed/local architecture that is not so much dependent on one central server location or network. Push model is usually preferred; however, pull is necessary for security reasons and handling of attachments.

4.2.2 Strategy Beyond Increment I

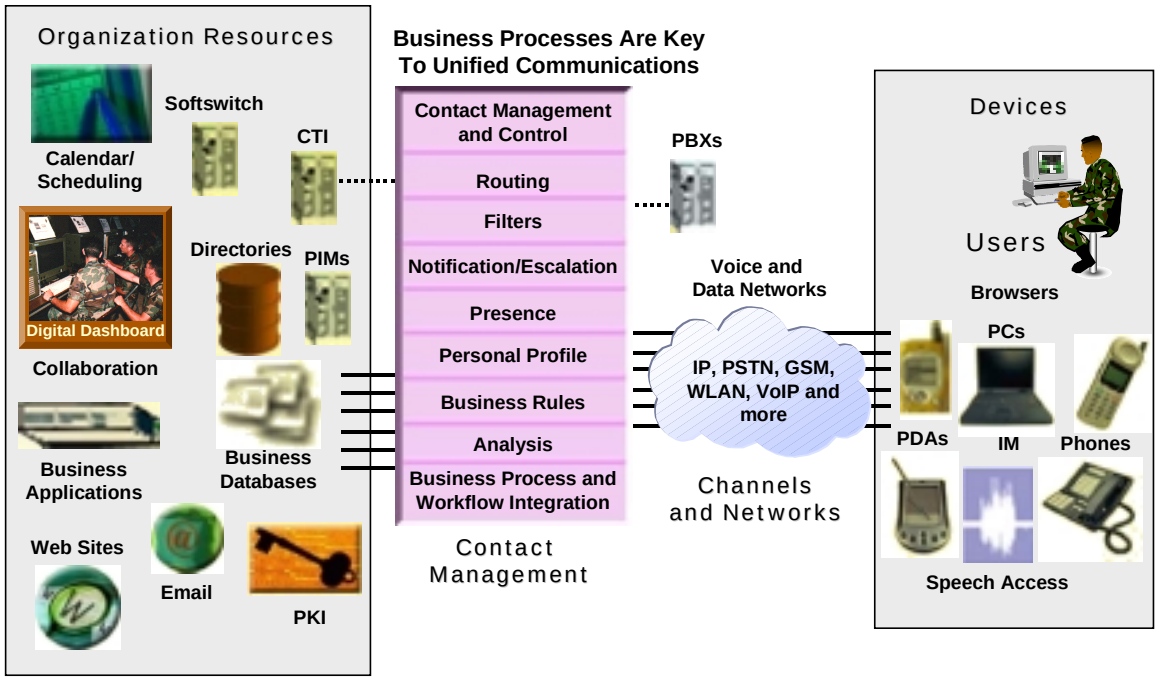


Figure 4.2.2-1 Unified Communications and Video Messaging (RTE)

In the longer time frame the technology trends will eventually lead to Unified Communications and Video Messaging due to the combining of Data Communications and Telecommunications to allow Real-Time Enterprise (RTE) capability. The System integrates Communication and Contact Management tools with all channels, and with business processes, applications, rules, and databases. Ultimately, unified communications is about business process improvement, not communications.

Unified Communications and Video Messaging (RTE)

In the longer timeframe technology trends will eventually lead to Unified Communications and Video Messaging due to the combining of Data Communications and Telecommunications to allow Real-Time Enterprise (RTE) capability. The System integrates Communication and Contact Management tools with all channels, and with business processes, applications, rules, and databases. Ultimately, unified communications is about business process improvement, not communications.

Interoperability and Global Communications

GES Messaging will need to provide enhanced interoperability and global communications among DoD Organizations, with other Government Agencies, the Intelligence Community, Host Nations and Commercial Facilities. There will be the need to interoperate with Allied/Legacy Systems and communicate across security domain boundaries. GES Messaging's integration with Translingual Services will be required for providing more effective multi-national and global communications.

4.3 Application

Application - Basic Capabilities

- Protected hosting environments
- Model Operating Environments (MOE)
- Computing capacity on demand
- Standard operational management and support

While DoD has made great strides in adopting, adapting to, and implementing Internet and web-based technologies and capabilities, the majority of DoD's distributed computing environment remains primarily a platform-centric world. In spite of efforts that have significantly reduced the number of data centers and types of computers that must be supported, today there remain a large number of combinations of hardware and software platforms in use ranging from obsolete mainframes and custom designed single-purpose computers to state-of-the-art web-enabled virtual data centers. In spite of efforts to encourage the adoption of "standard solutions" IT solution developers are still largely free to make their own selections of specific hardware, operating system and functional application software with little view towards the impacts their selections might have on DoD as an enterprise. Developing and deploying GIG Enterprise Services (GES) presents a unique opportunity for DoD to further reduce and consolidate the number and types of computing platforms that must be Operated and Maintained (O&M).

The Application service is fundamentally about establishing a "network" of enterprise computing service providers capable of supporting GES Core Enterprise Services (CESs) and Community Of Interest (CoI) applications and services throughout their life-cycle. The service will provide protected operational hosting environments consisting of common hardware platforms, operating systems, and core applications that will be used to host CES and CoI services. The Application service will take a more structured approach to CES and CoI hosting by adopting a concept called the server Model Operating Environment (MOE). MOEs will consist of one or more suites of hardware platforms and preferred software tools that would provide a common environment for developing, testing and operating functional applications. Each suite would consist of operating systems and hardware platforms offering an agreed upon levels of computing capability, standard third-party software and versions and a common storage infrastructure. The value of a MOE is that the use of a target design and operational environment will lead to increased availability, improved interoperability, and reduced development costs. In addition, by building on standard information processing techniques, accepted industry best-practices, standards for assured computing, and proven Application Service Provider (ASP) services, the Application service will establish standard sets of operational processes and procedures that support the CES/CoI life-cycle, further reduce O&M costs and provide levels of support.[1]

The Application service will focus on providing: 1) MOE-based protected hosting environments for all security levels; 2) ESM service implementations for monitoring, managing, controlling, and load balancing hosted applications across geographically dispersed sites; and 3) a staging service to stress test enterprise applications prior to operational deployment and 4) implementations of ESM Configuration Management (CM) and Software Distribution (SD) services to ensure that upgrades and changes are consistently made both within and across sites.

[1] Model Operating Environment (MOE) concept has been adapted from a draft whitepaper by Mr. John Garing (Principal Director DISA Computing Service) and Ms. Dawn Meyerriecks (DISA Chief Technology Office).

4.3.1 Strategy For Increment I

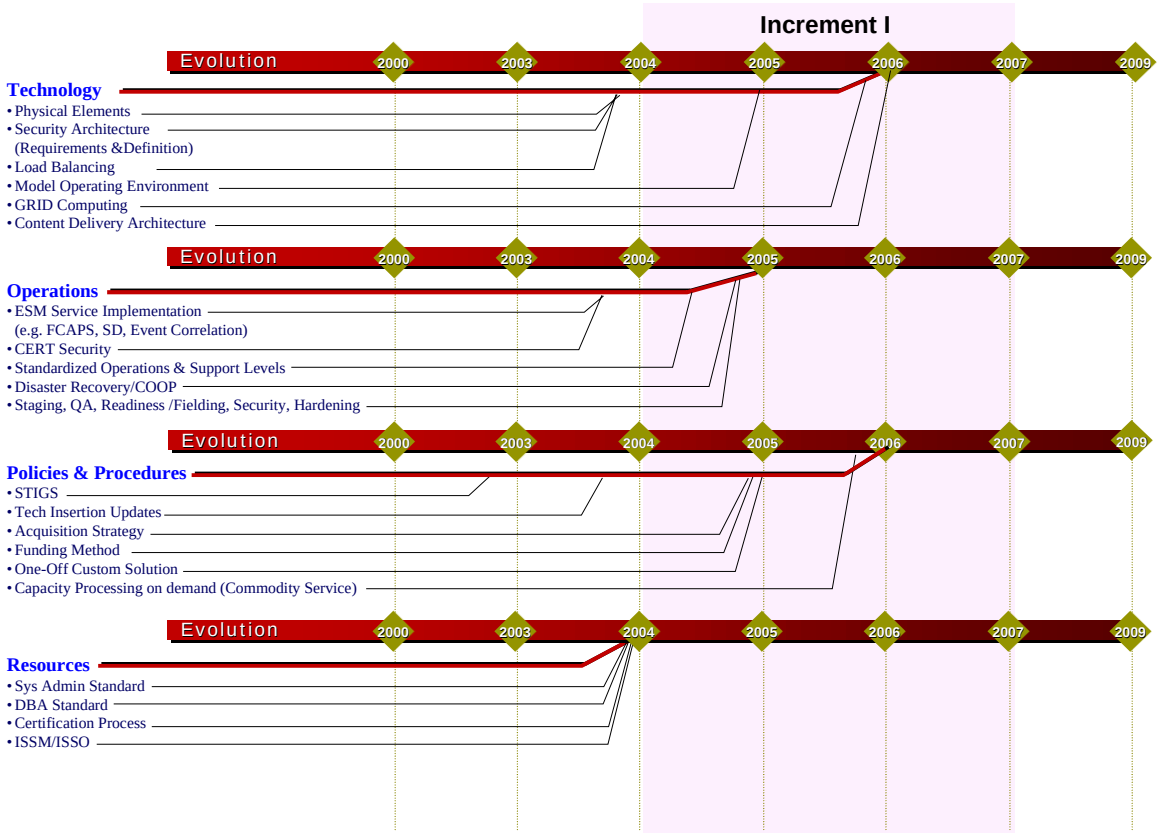


Figure 4.3.1-1 Application Service Evolution

Technology

Application hosting service facilities must have an extremely robust and flexible network and security architecture capable of simultaneously supporting and enforcing the wide variety of networking requirements and security policies that will need to be implemented by the various CES and CoI services. Facilities must ensure that all data and information is afforded the necessary degrees of protection while in transit, at rest, being processed and that data can only be accessed by authorized services or individual users. It is anticipated that the internal Local Area Network (LAN) infrastructure of the Application hosting service facilities would be based on Gigabit-Ethernet with multiple redundant and independent network connections being provided by the GIG-Bandwidth Expansion program. Application service protected hosting environments will employ multi-layered Defense-In-Depth approaches that provide the necessary network, enclave, host, and operating system level protective mechanisms through the smart implementation and use protective mechanisms such as firewalls, anti-virus technologies (AV), virtual private networks (VPN), intrusion detection systems (IDS), and Security Technical Implementation Guides (STIGs), to limit and control logical data and information access, as well as sound physical security protective implementations that will limit and control physical access.

The Model Operating Environment (MOE) is the center-piece and core of the Application service. MOEs will consist of one or more suites of hardware platforms and preferred software tools that will provide a common environment for developing, testing, staging, deploying, and operating GES services and functional applications. Each suite would consist of operating systems and hardware platforms offering agreed upon levels of computing capacity, standard versions of selected third-party software

applications, and a common storage infrastructure. MOEs would be offered at agreed upon service levels and prices to CES and CoI service developers. This model would allow for the establishment of increased commonality across the DOD computing infrastructure without having to select one single platform. Critical to service developers, moving to a MOE-based computing environment should also significantly reduce or eliminate the need for them to individually negotiate for the deployment and support of services or applications at multiple locations. It is expected that MOEs will be developed and offered for selected mainframe computers, several varieties of Unix, Windows, and Linux operating systems. Support for major database applications will also be provided as well as support for Enterprise Resource Planning (ERP) solutions.

Operations

As already notes, the implementation of ESM service capabilities will be absolutely essential to successfully operating and maintaining the GES Application service. Implementations of ESM services and capabilities such as fault, configuration, accounting, performance and security (FCAPS) management as well as robust and sophisticated event correlation, management, and assessment capabilities will be an integral part of the Application service. Successfully responding to user and customer concerns and problems on a 24x7x365 basis will also require well defined service desk capabilities at Application service provider locations.

Critical to large-scale operations of this type will be the ability to do automated software distribution to ensure that: 1) consistent builds of application software are deployed; 2) patches are consistently and properly applied as part of the overall security architecture; and)3 all installed software complies with applicable Information Assurance Vulnerability Alerts (IAVAs).

By simulating the load imposed by the anticipated customer base, the application or service testing, staging and deployment portions of the Application service will allow material developers to test and stage their products in a real-world setting therefore providing them with a much better picture of how they will operate in the production environment or MOE that they have selected. The staging service will also provide a much more cost effective way of moving new or updated/upgraded services into production. To ensure consistency and continuity within and among operational facilities, the application service will also provide a Configuration Management (CM) service offering as well as a Quality Assurance service.

Finally, changing both the technical approach and the business approach should allow the Department to develop a Capacity On Demand capability whereby computing capacity is added at a rate that at least equals projected requirements to include identified surge requirements. In this manner, if a particular Community of Interest were to experience some unforeseen requirement for additional computing capacity it would be readily available. It would also preclude the requirement for every developer to have to plan and build for a maximum capacity and fail-over scenarios, when in fact, a coordinated fail over and disaster recovery plan is more effective than having each application provider develop their own uncoordinated plan.

Policies and Procedures

Deploying and operating most if not all of the proposed CES and CoI applications and services will require changes to existing DoD, Combatant Command, Service, and Agency policies and procedures and the Application service is no exception. DoD is a culture where the ability to exercise direct command and control of the critical resources needed to prosecute the mission is the accepted norm and any model that attempts to change the norm is typically met with varying degrees of resistance. The Application service concept is a logical extension of past and current efforts that have successfully consolidated computing resources from across DoD. Continuing and expanding this process can only serve to further improve DoD's computing capabilities, reduce costs, and provide enhanced levels of support to the warfighter.

Policies that mandate the use of specific combinations or types of hardware and software have generally enjoyed only marginal success and have not been widely enforced, e.g. Ada. The approach for GES will be to develop and implement policies and procedures that make it more attractive from cost, schedule, and operational mission perspectives for a GES service or application developer to use a MOEs provided by an Application service provider than it would be for them to develop their own individual solution.

Resources

The move to an Application service provider model will almost certainly require changes to current DoD IT business models, to acquisition strategies, and to the way in which DoD funds for IT investment and operations. This includes funding and maintaining the physical infrastructure, facilities and personnel to support enterprise-class application hosting and support facilities in the locations where they are needed both in CONUS and in selected overseas locations as needed. Maintaining and operating an infrastructure of the type envisioned under this service will require significant capital investment and capital refresh just to keep pace with advances in technology and requirements for increased capacity. It would in all likelihood require some form central funding for the Application service along with a model to allow for cost recovery or fee for service operations. Rather than having each material fund for and deploy individual computing infrastructures, the Application service model would have a material developer select an MOE and then fund an application service to provide the capabilities and capacity that they need.

In addition, successfully deploying, operating, and maintaining the dynamic operational environment that the Application service will support places an increased premium on attracting, training, and retaining a world-class workforce with cutting edge technical skills in a wide variety of areas including distributed database design and management, operating system administration, and network and host platform security.

4.3.2 Strategy Beyond Increment

Since the Application service is core to the development, testing, and deployment of Core Enterprise and Community of Interest applications and services it must be front-loaded into the GES development process. If the Application service is not developed and deployed early in the overall GES life-cycle, DoD runs the risk of continuing the current approach whereby material developers would continue to develop custom solutions designed to meet their specific set of requirements. Breaking that model requires a fundamental change in how requirements are addressed and in how applications and services are developed, deployed, operated, and maintained. Beyond Increment I the strategy for the Application service would be to embark on a continuous process of smart technology insertion and refresh using a controlled process to ensure that a stable, robust, managed and secure application infrastructure is established and maintained for the long-term.

4.4 Discovery

Discovery - Basic Capabilities

- Data source discovery
- Content management
- CoI ontology management support
- Knowledge bases

The Discovery service is a key element in enabling the transformation to net-centric information technology services and capabilities. The discovery service provides visibility and access to information and services available in the Net-Centric environment. While many exchanges of information and uses of services will be predefined, it is also important for information and services to be usable for unanticipated users and applications. This flexibility will be essential in the "many-to-many" exchanges of a net-centric environment. While tightly engineered, predefined interfaces between systems will continue to exist (e.g., sensor-to-shooter systems), the objective in a net-centric environment is to increase the potential for many other systems to leverage the same information and capabilities without having to anticipate this use in the development cycle. In an environment in which systems are continually being developed, deployed, migrated, and replaced, making allowances for unanticipated interfaces is essential. The Discovery Service provides that essential link between providers of services and the end-users that consume them.

4.4.1 Strategy For Increment I

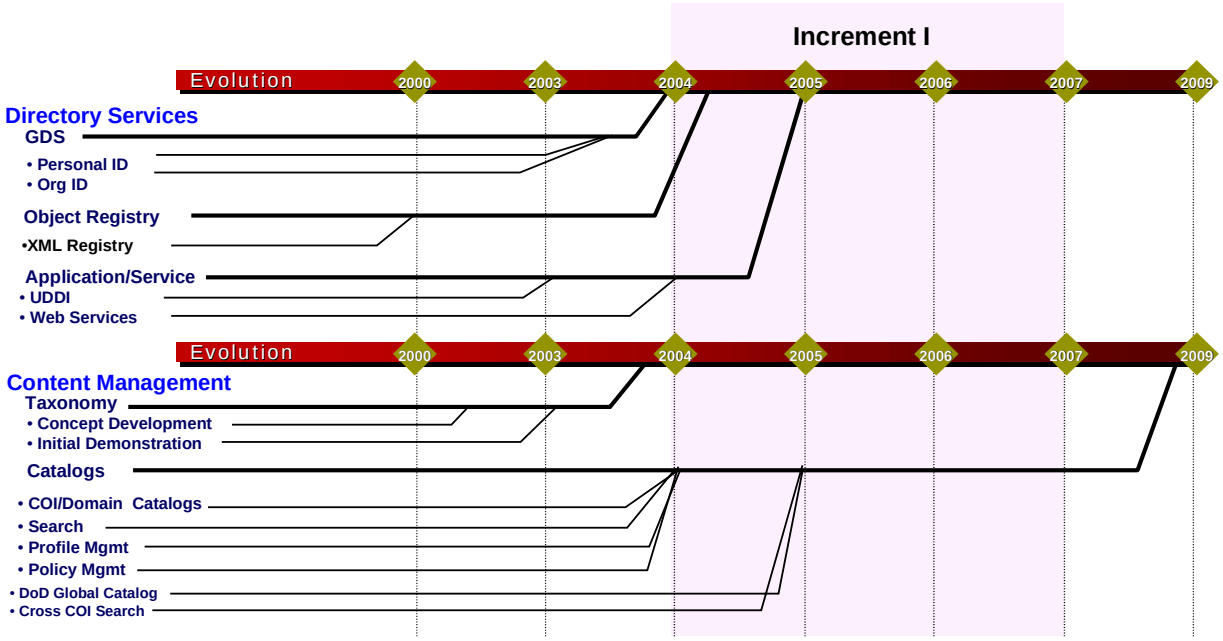


Figure 4.4.1-1 Discovery Evolution

Directory and Registry Services

GES Discovery services provide the core capability to allow GES capabilities to scale to the full global scope of DoD's environment. Discovery services remove the responsibility from individual users to develop information infrastructures to enable interactions within a networked environment. The dynamic nature of information resources and services in the GIG also make it impractical for individual users (or organizations) to maintain an awareness of the information and services available across the enterprise. The directory and registry services will provide the necessary information, while masking the underlying complexity of the infrastructure. The actual repositories for information will be provisioned through the storage and application CES, but the creation, management, and maintenance of meta-data and the services to catalog and search those repositories are provided by the Discovery CES.

During Increment 1, GES Discovery services will be focused on enabling the transformation of localized capabilities to enterprise resources. The initial capabilities will evolve from current directory and registry activities. Visibility of information resources will be supported by metadata registries, providing 'build-time' information (e.g. data structures and syntax) to application developers. In addition to metadata, other directories and registries will support the discovery of information on people, organizations, and services. During Increment I, most capabilities will need to be replicated in each security domain, until appropriate cross security domain services are available. As these become available, and provide the capability to share information across the security domain boundaries, duplication of content can be reduced.

Content Management Services

Content management services enable information and service producers to define, create, manage and maintain metadata about their information and service capabilities. Catalog Services provide information producers with services to characterize their products using metadata, and store the metadata in a catalog in accordance with a predefined set of fields and attributes (schema). Initial capabilities will provide support for text based information sources, evolving over the span of Increment I to other information resources and formats (e.g. imagery, geospatial, etc.). During this time frame, the primary responsibility for cataloging will rest with Domains and COIs; the Discovery CES will provide services that may be used by Domains and COIs to build their catalogs and indexes, and to provide search capability across the GIG. These service will also be extended to provide visibility and access between CoIs and Domains, and across security domains. As the cataloging service evolves, it is also important to manage the semantic content of the catalogs, and to capture the ontologies and taxonomies within communities. This will evolve over time to include the necessary transformation and mapping between CoI ontologies to improve data interoperability.

Search services leverage the cataloging services to allow users to identify and access information in their local infrastructure and beyond. A search may be an ad-hoc query, or an automated retrieval or distribution of information products. Initial capabilities will be similar to current Internet search services like Google, this will be augmented by profile services. This will allow users to establish a profile for each information product they require by specifying what the product is and where it is located, and when and how they need to access it.

Ontology Services

The ability to find and categorize the wide variety of content on the net will be a critical enabler for end-users trying make effective use of an array of data offerings. Ontology management tools provide the facilities that data service providers will need to set up and evolve enterprise ontologies. (IEEE 2003) Additionally, the tools provide the means for defining mappings between autonomous ontologies. Terms and implied semantics have naturally evolved in the CoIs in independent and sometimes contradictory ways. Standardized community ontology specializations will enable end-users to more efficiently navigate the wealth of DoD data offerings.

Operations, Polices, and Procedures

The Discovery service provides capabilities to both end-users and to other CES and CoI services. It is used by most of the other CES' to enable their interactions with other services, and to make their capabilities visible and accessible to consumers. The key changes from current operations to initial Increment I/Spiral 1 Discovery services is the evolution from separate application, Service, and CoI implementations to DoD-wide, integrated solutions, providing shared services and consistent interfaces to all users. DoD has established new directions in its Data Management Strategy, and is developing new guidance for developers and users to reflect the shift to a Net-Centric environment. Similar changes in policy will be required to support other aspects of the Discovery service, including guidance on publishing and controlling service interfaces, and personnel and organizational information.

4.4.2 Strategy Beyond Increment I

Since the Discovery service is core to the development, testing and deployment of Core Enterprise and Community of Interest applications and services it must be front-loaded into the GES development process. If the Discovery service is not developed and deployed early in the overall GES life-cycle, DoD will not be able to reap the full benefits of a service oriented, net-centric environment. Beyond Increment I the strategy for the Discovery service would be to embark on a continuous process of technology insertion and refresh using a controlled process that will enable the evolution of the net-centric environment from statically configured service interactions, to a dynamic environment supporting run-time discovery and association of information and services from a variety of service providers, for delivery on demand to consumers.

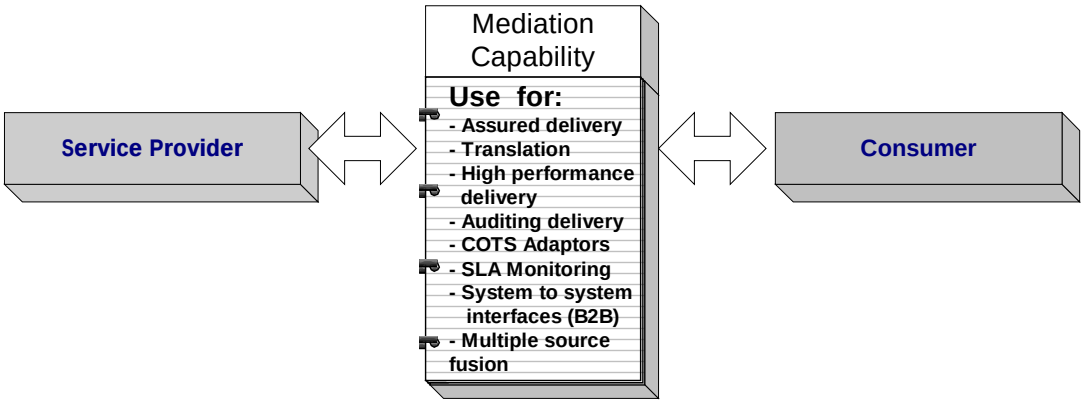
4.5 Mediation

Mediation - Basic Capabilities

- Assured delivery, auditing of delivery
- Conversion, fusion of content
- Data translation
- B2B support
- Enterprise Application Integration (EAI)
- Business Process Management

Mediation is a middle layer of processing between producers of information and consumers of information. Mediation provides automated capabilities for assured delivery, translation, conversion, fusion and routing of information between participants. Mediation is an optional service between two parties who choose to use it because it offers them value.

Operational services on the net can be created by service providers in a mediated or unmediated form. Unmediated services do not use this CES and allow direct connection from the consumer to the service provider. As depicted in Figure 4.5-1, systems that decide to use mediated services make use of a **third-party intermediary that provides a range of additional capabilities** including guaranteed, complete, once-and-only-once delivery, scalability and fail-over of interactions, data translation, business process integration and business rule creation and execution, and use of standardized information assurance capabilities.



4.5-1 Mediation's Role As A Third Party

Mediation of services is a long-term activity that spans the useful life of the service. Mediation may occur from both the consumer and provider perspective. The key to understanding service mediation is recognizing that within the operation of a service, many individual transactions occur. These interactions, if they are deemed worth the resources and expense, can be carefully monitored, audited, and protected to provide a number of benefits, such as:

- "Transactional" guarantees of assured, once-and-only once message delivery
- High performance, "out-of-the-box" mapping and integration components
- Ability of process owners to track transactions under mediation
- Detailed statistics and auditing of all interactions
- Secure encrypted transport with DoD Public Key Infrastructure (PKI) based authentication and non-repudiation
- Alerts for interactions that fail certain performance thresholds

Mediation also includes auditing transactions to give both providers and consumers of services an *aggregate* view of what is being provided and consumed. For example, this aggregate information can be used to provide compensation to providers, if the provisioning model provides for a fee based on use. The information can also be used to make decisions on the enterprise portfolio based on actual service usage as measured by a neutral third party.

Services may also be run in an "unmediated" mode, where there are direct flows of interactions between the consumer and publisher's systems with no oversight or intervention. This may be a reasonable option for consuming services that are not critical, or are anonymously given away without charge.

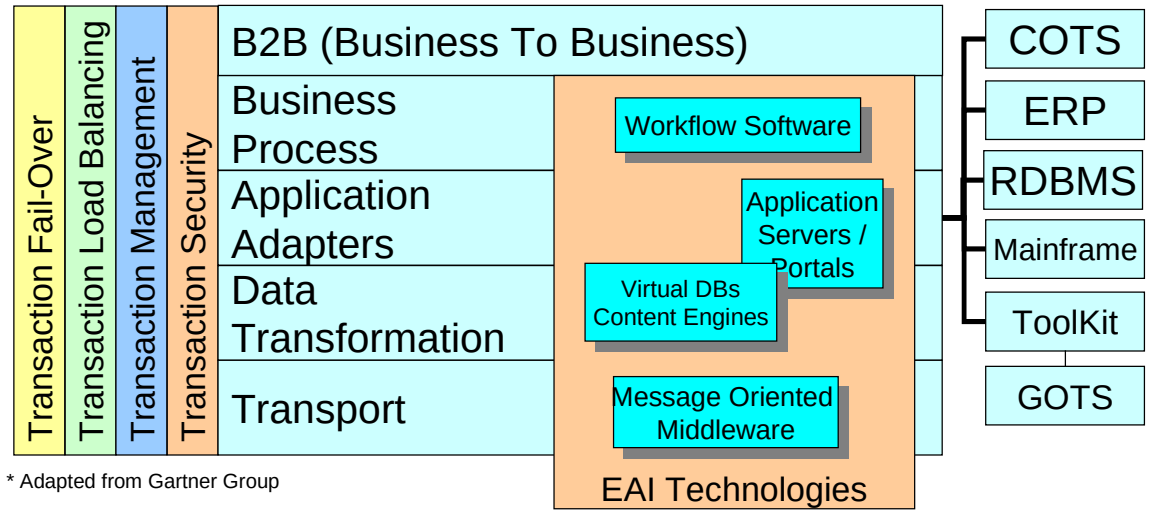


Figure 4.5-2 Notional "Stack" of Mediation Capabilities

As depicted in Figure 4.5-2, Mediation is a service is provided by a stack of functionality that may be deployed throughout a network or located in specific network locations. The mediation functional stack must be comprised of at least transport and data transformation capabilities. Transport includes message queuing, and publish and subscribe functionality with an option to be fully *Atomicity, Consistency, Isolation, and Durability* (ACID) transactional. Data transformation must allow for rapid any-to-any conversions, centering on XML but supporting other legacy formats such as user-defined flat files and Electronic Data Interchange (EDI). Application adapters may be added on top of data transformation to provide flexible and powerful connection to network based systems including legacy systems such as mainframes. Business Process Management (BPM) may be added on top of application adapters to provide for flexible management of messages between systems and optionally to people. Finally, a B2B layer may be added to facilitate limited and secure information exchanges between businesses or organizations. Integration Brokers, Virtual Databases, Content Integration Servers are examples of Commercial Off The Shelf (COTS) Enterprise Application Integration (EAI) products that have been focused on mediation.

There are two important axes for characterizing Mediation. The first is whether the mediation function is synchronous or asynchronous and second is whether the mediation processing location is distributed or central.

A central synchronous Mediation CES will access and fuse data on demand, and return a result to the consumer, often within a few seconds. This CES will be operating at redundant network locations to provide a good level of availability, and provide fail-over within seconds. Distributed synchronous Mediation GES represents a future path for the maturation of central synchronous Mediation CESs. It will potentially provide better availability and performance by distributing and managing the execution of mediation processing across the network.

A central asynchronous Mediation CES can, from queues and/or in batch, provide a set of data transforms and routings to transactions that can serve machine-to-machine business processes. Electronic Data Interchange is a mature and continuing form of this service. This CES will be located at multiple locations to provide a good level of availability, although its CES fail-over time is based on Service Level Agreements for delivery times (often 24 hours). A distributed synchronous Mediation GES deploys the processing of data transforms and routings of objects and messages across the infrastructure, near to the producers and consumers of services. This provides for better performance and availability.

For the sake of simplicity, all these mediation options are all rolled into the Mediation CES, which may be created from more than one class of COTS, depending on the best solutions available at deployment time. These mediation services will become available incrementally as they mature and are consistent with the level of service offering consistent with CES. This timeline is shown in Figure 4.5.1-1.

4.5.1 Strategy For Increment I

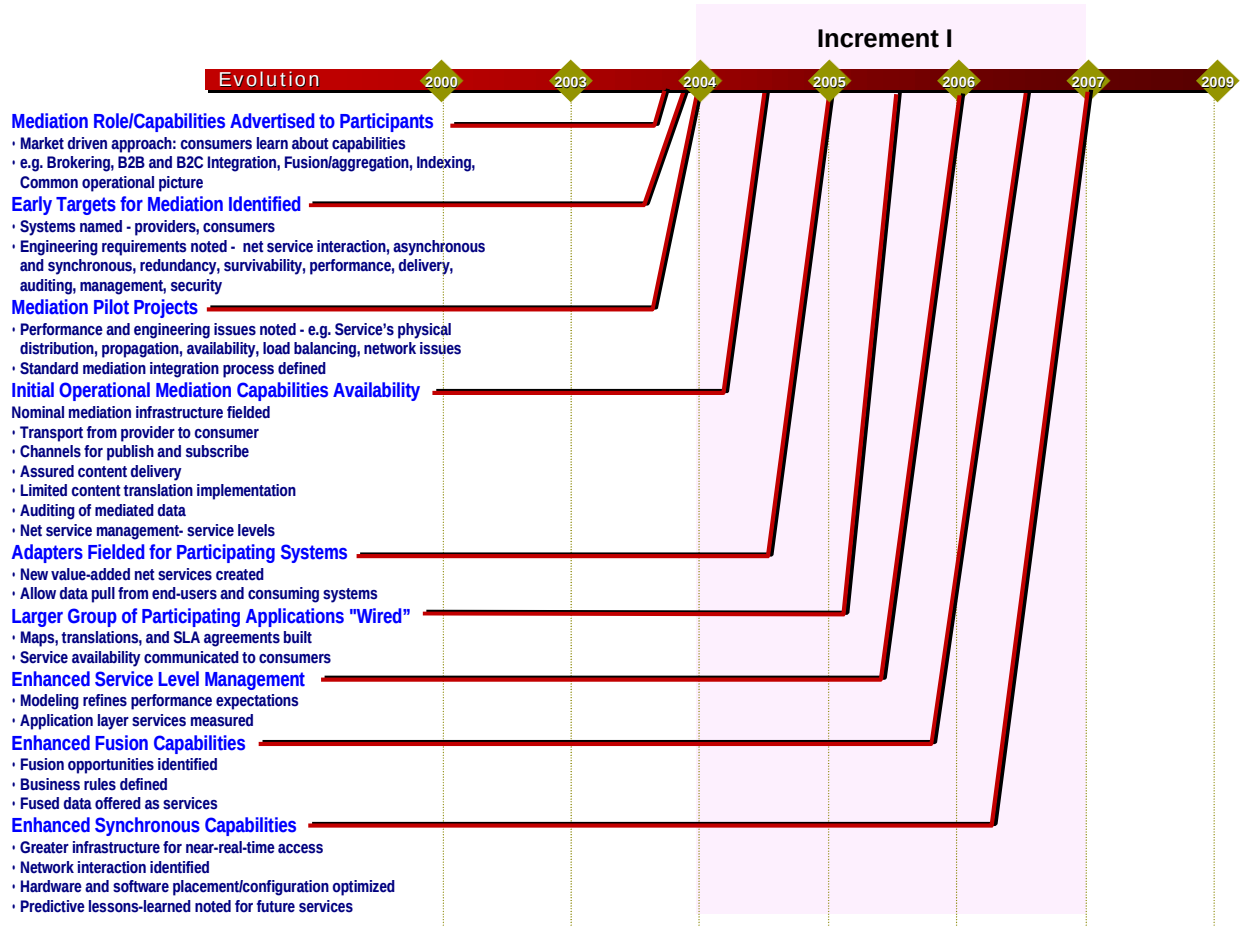


Figure 4.5.1-1 Mediation Evolution

Mediation Role/Capabilities Advertised to Participants

Since mediation for many will be considered an optional service, a initial period of capability education, advertisement and feedback collection will be needed to set up the original collection of information publishers and consumers.

Early Targets for Mediation Identified, Mediation Pilot Projects

Once a small set of publishers and consumers have been identified, engineering requirements including net service interaction, asynchronous and synchronous needs, redundancy, survivability, performance, delivery, auditing, management and security are created. Then, in conformance to the development of other GES, performance and engineering issues (e.g. Service's physical distribution, propagation, availability, load balancing and network issues) drive initial designs. These designs are then normalized to define a set if standard mediation integration processes.

Initial Operational Mediation Capabilities Availability

During this step a nominal managed mediation infrastructure is fielded with minimum service levels. These services include transport from provider to consumer including channels for publish and subscribe and assured content delivery. Limited content translation implementation is enabled, such as to, from and between XML and flat files. Auditing logs of both transported and translated data will be made available via a web portal and as XML based reports, aiding customer self-service for a variety of tracking and reporting needs.

Adapters Fielded for Participating Systems

Mediation services become more useful after the adaptation of systems to the infrastructure. Through use of the application layer adapter, both synchronous and asynchronous applications can be addressed directly through the data transformation, transport and business process management layers, creating a unified way of addressing a number of applications. Legacy, Government Off The Shelf (GOTS) and COTS applications can be added with various flows and logical routings creating new value-added net services.

Larger Group of Participating Applications "Wired", Enhanced Service Level Management

Application performance management of both the mediation infrastructure and the participating systems along with modeling of wide scale performance allows higher quality Service Level Agreements (SLAs) to be created. New systems services, additional transformation options and high quality SLAs are then communicated to current and potential service consumers to stimulate demand, and lower the variable costs for all.

Enhanced Fusion Capabilities, Synchronous Capabilities

Data and information fusion can be a processing intensive activity. As the mediation infrastructure matures and is enhanced, and the number of systems adapted to the infrastructure grows, additional cross-system fusion opportunities are created. Users can leverage web portals to directly enter business rules to fuse the various sources to create new services. These services can be chained asynchronously, or if a higher level of infrastructure investment is made, perform in a near real time, synchronous mode. In either case, observation and deployment of demanded processing nodes across the network allows optimal use of resources which facilitates near real time fusion services.

4.5.2 Strategy Beyond Increment I

In the long run, although the infrastructure for mediation may mature, research may add additional options for higher quality data fusion through advanced algorithms, agents or various machine intelligence approaches (neural networks). Increases in bandwidth and processing speed will enable ever better use of the mediation infrastructure.

4.6 Collaboration

Collaboration - Basic Capabilities

- Shared workspaces, whiteboards, and applications
- Supporting audio, video, and chat

Collaboration is one of the Core Enterprise Services (CESs) within the Global Information Grid (GIG) Enterprise Services (GES). It complements other services such as Messaging, Mediation and Discovery to provide a comprehensive access to information from anywhere, anytime, over any medium, and from any device or application. The CES of Collaboration will provide users with a range of interoperable collaboration capabilities, based on commercial standards that are secure and fulfill DoD's operational requirements. This will be an enabler ensuring real-time situational updates to time critical planning activities between joint, coalition partners, the Intelligence Community, and Agencies at all levels (DoD, Federal, State, and Local). Levels of collaboration include Awareness, Shared Information, Coordination and Joint Product Development. Historically, Collaboration Services were handled via Meetings, Conference Calls, Email and Newsgroups. Real-time collaboration has been provided through point solutions, which have been unable to support the DoD dynamically. As this technology evolves a great deal of synergy will be seen between the CES of Collaboration and Messaging. Currently, the services-based components include the following capabilities:

- Chat/IM – Holding a text conversation with other members in the same conference.
- Whiteboard – Sharing a simulated drawing space with other users. Can be used to annotate pictures or maps.
- Audio – Sharing audio among users in a conference.
- Video – Sharing audio and video among users in a conference.
- Shared Applications – Allowing any application running on a user's machine to be shared with all other users in a synchronous meeting session, even if they do not possess the application. Sharing gives users the ability to either view the application or to both view and interact with the application.
- File Sharing/Virtual Workspace – A persistent environment equipped to hold and support user meetings and import and store multi-format information products for later retrieval and use.
- Awareness – Application that provides users of different systems (i.e. Defense Collaboration Tool Suite (DCTS), Oracle Collaboration Suite (OCS), Collaboration Virtual Workspace (CVW), InfoWorkSpace (IWS), Sametime, CUSeeMe, etc.) awareness or presence of users and spaces.

In the near term, DoD Collaboration requirements and standards are continuing to evolve and mature while technology trends are being assessed. Web Conferencing and Instant Messaging (IM) are increasingly being used in the enterprise to enable people to communicate, collaborate and learn in real time. Publish/Subscribe and Web Services will provide quick registration/access, cross enterprise awareness and enhance interoperability among DoD organizations' portals. The combination of data communications and telecommunications will result in Unified Storage and Unified Communications through Internet Protocol (IP) channels and devices. Translingual Services will help to improve communications for interaction with our coalition partners. In the long run, Collaboration standards will continue to mature while the necessary components will migrate as they prove to be part of core infrastructure for GIG ESGES Collaboration Services. Collaboration functionality will be embedded into applications that will provide improved Information Management, Knowledge Management and Functionality for different Communities of Interest (COIs). Reliability, Security, and Interoperability among GIG ESGES Core Services (i.e., Messaging, Discovery, Mediation, User Assistant, etc.); across domains, multi-security levels/networks, along with scalability and performance are some of the

challenges and crucial objectives that this collaborative environment must achieve. Collaboration should be fluid, allowing teams to form rapidly and dissolve across time, space, and Agency and Service boundaries.

4.6.1 Strategy For Increment I

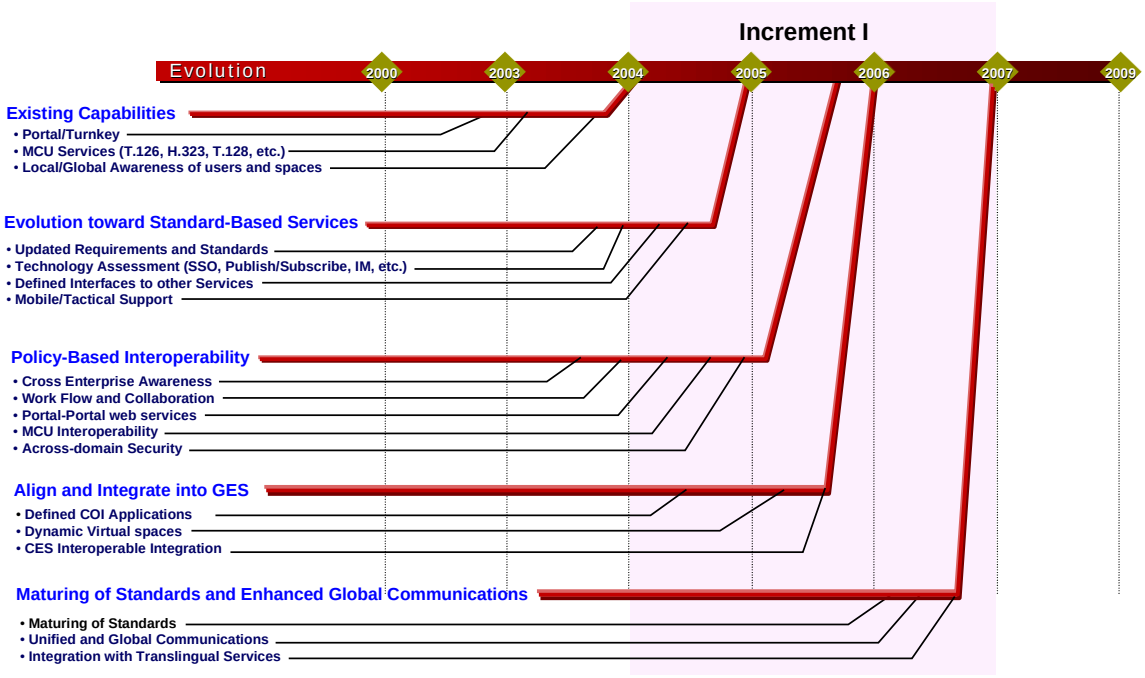


Figure 4.6.1-1 Collaboration Evolution

Existing Capabilities

DoD has directed the use of NetMeeting/SunForum as a construct for the basic building block for DoD's collaboration strategy. *"This will set the stage for a cooperative effort where government and industry can come together to help shape the way for a fully interoperable, multi-vendor collaborative environment."* Additionally, the DoD has directed that all collaboration products utilized by DoD must demonstrate compliance, interoperability, and certification by Joint Interoperability Test Command (JITC) before they can be used on DoD networks. The current collaboration initiatives utilize a fully featured suite of Collaboration tools that consist of many parts including NetMeeting, SunForum, Digital Dashboard, CUSeeMe, Envoke, Streaming Server and RealPlayer. This capability has Portal/Turnkey, Client/Server, N-tiered (partial), Thick Client and component services (Audio, Video Multipoint Conferencing Unit (MCU) H.323, Shared application/whiteboards [MCU T.120], File Sharing/Virtual Workspaces). Collaboration integrates with other services such as Local/Global Directory, Public Key Infrastructure (PKI), Messaging and Awareness. The current initiatives are still evolving in the area of Enterprise and Persistent Chat, Large One-to-Many collaboration, Single Sign On (SSO), etc. This will be enhanced with the widespread and expanded implementation of Envoke, Multilingual Translation, Groove Integration and DoD PKI. The current approach utilizes a sophisticated design which is establishing a flexible architectural approach which allows the ability to change-out components as the technological baseline evolves. The challenge is to establish a collaborative environment that allows any interoperable platform to collaborate/interoperate with authorized users. This will provide a reference implementation/baseline to be followed as a logical transition point from legacy approaches to the GES. Additionally, it will provide a logical path as

Collaboration and Messaging converge. The existing Collaboration capabilities are technically outdated, expensive, have serious security flaws and do not scale well. There is the need to continually look at collaboration technology trends and potential redesigns and/or enhancements to make Collaboration the GES. Security, interoperability standards, global awareness and communications need to be expanded and improved.

Evolution toward Standards-Based Services

In the near term, Collaboration service's requirements and standards are to be revisited and updated. The CoI applications and DoD mission needs will be the main drivers. Security/Privacy/Management should be well thought out up front. Current technology will be assessed along with its evolving trends. Secure collaboration is an elusive goal, which necessitates comprehensive technological, business, and legal frameworks to govern widespread, interoperable, multi-vendor solutions. The DoD must ensure the evolution path embraces all the collaborative environments spanning messaging, conferencing, ad-hoc document sharing, and other related applications and services. Below are some of the key enabling technologies, features, and capabilities, which will provide the integration and enhancements for the needed services. Some of these features and capabilities may be provided by augmenting other CES such as Messaging, Mediation , ESM and Discovery.

- Web Conferencing (e.g., Webcast, WebEx) and IM are increasingly being used in enterprise to enable people to communicate, collaborate and learn in real time.
- Publish/Subscribe Services are becoming the communication models.
- Enhanced Visualization via Whiteboard T.126 and Non Destructive overlays.
- Crossing infrastructures with Video Tele-Conferencing (VTC), Telephony and Mobile/Wireless/Handheld networks.
- New Concepts for interoperability via Web Services.
- Thin Client (HTML, WAP, futures).
- Browser Client (HTML 3 [portal, Envoke], MS DD portal, HTML 4 and XML, portal agnostic).
- Peer-to-Peer communication is another type of data-oriented synchronous environment collaboration architecture, which relies on a fat client at the desktop.
- Scalable deployment to provide support to growing enterprise messaging and other collaboration-related traffic, including premises-based versus externally hosted and centralized versus decentralized server deployments.
- Dynamic Conference Scheduling.
- Work Flow capability can be improved.
- Real-time network and system status.
- Alert capability needs to be improved.
- Group Authoring, Group Personal Information Manager (PIM) (Calendaring and Scheduling).
- Global Awareness of users and spaces needs to be improved.
- Streaming Broadcast Service such as Real Player and Streaming Server.
- Standard Operating Procedures (SOPs) and Tasking.
- Translingual Services will be implemented to provide more effective global communications.

The CES of Collaboration will evolve to include synchronous collaboration services, browser-based collaboration services, ad-hoc, and virtual shared workspaces. It will rely on other CESs to provide knowledge management and secure messaging services.

Collaboration Services will need to interface with DoD common infrastructures such as Global Directory Service (GDS) and DoD PKI, and other CES such as Discovery, Mediation, Messaging, and User Assistant Services. The Collaboration components that will evolve toward Standards-Based Services include:

- Shared file space of New Technology File System (NTFS) will move toward URL-based reference.
- Audio will bridge to Session Initiation Protocol (SIP) based, H.323, InfoWorkSpace (IWS) Placeware1 and IP Telephony.
- Video will bridge to SIP-based and H.323 IP Service.
- IM will evolve toward Internet Engineering Task Force (IETF) IM and Presence Protocol (IMPP) (SIMPLE & CPIM).
- Whiteboard (T.126, futures).
- Shared Applications bridges to T.128 futures.
- Envoke (GOTS) Awareness bridges to IETF Standard (SIMPLE, futures).

The CES of Collaboration will effectively support our warfighters in a mobile/tactical environment with survivable, lightweight wireless/wearable mobile devices. Ease-of-Use User Interface (UI), Interactive Radio Telephony (RT), Graphics, Audio/Video conferencing, off-line mode and bandwidth conditional operations, Data Compression, Security and Thick/Thin Clients are among some of the features to be considered for improvement. Until major mobile collaboration products mature, middleware gateways will be required to provide infrastructure features such as protocol conversion, content rendering, and session encryption.

Policy-based Interoperability (minimized GOTS)

Collaboration Interoperability will be extended across domains, organizations, and coalition partners. Cross-Enterprise Awareness will be the crucial component. Work Flow and Collaboration within different CoIs are to be worked out. Portal-Portal Web Services will be the mechanism to provide interoperability among different systems, applications and Common Operating Environments (COEs). Multipoint Conferencing Unit (MCU) interoperability has to be established. Cross-domain security policy hopefully will not be an obstacle for progress. These services will enable Secure/Private/Mobile delivery over heterogeneous infrastructures.

Collaboration Services will bridge toward Policy-based Interoperability with Single Sign-On (SSO), Access Controls across organizations/domains, and Multi-level security/networks. These security capabilities will be provided by Security Services. Security services will provide a robust end-to-end encryption, digital signature, archiving, and other key security features. Services will block unwanted content allowing users to filter and handle incoming, outgoing, and stored content. CES of Collaboration will provide interoperability and global communications.

Align and Integrate into GES

Collaboration components will interact with other CESs. This CES will support interoperable bridges, extensions, and will migrate to a family of interoperable tools. Collaboration functionality will be embedded in CoI applications and will provide significant improvement to Information Management, Knowledge Management and other functions. Collaboration CES will facilitate various styles of

distributed collaboration, including synchronous, messaging-based discussion threads; synchronous, conferencing-based communication sessions, including IP telephony; and ad-hoc, virtual work spaces.

4.6.2 Strategy Beyond Increment I

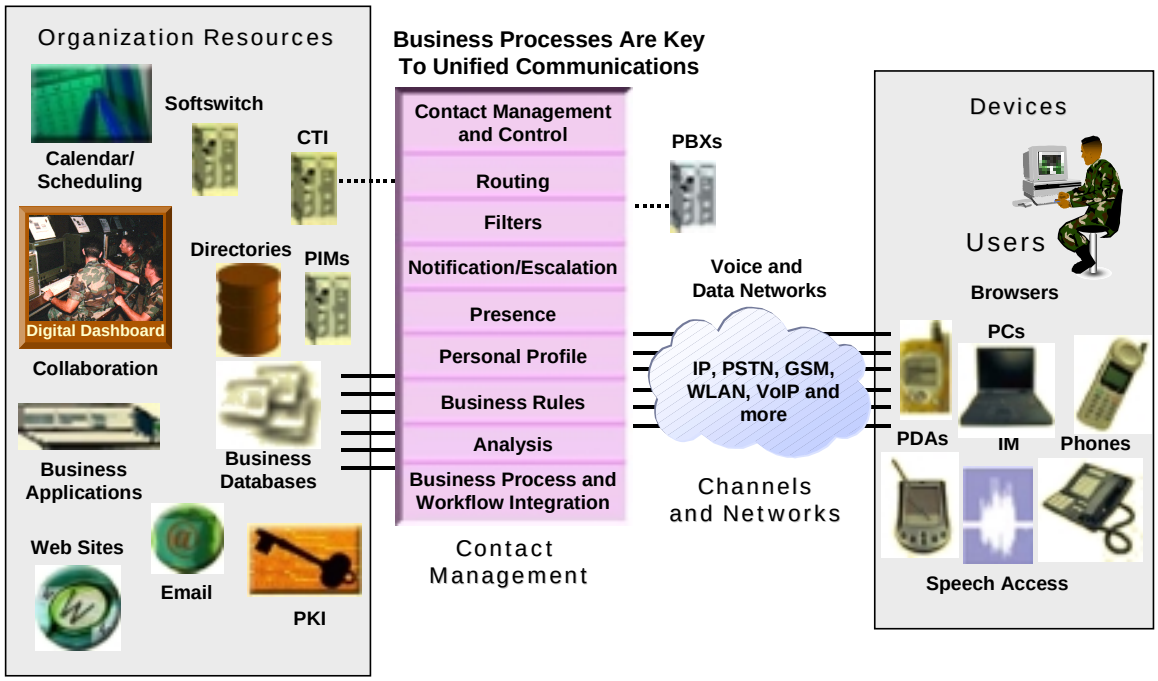


Figure 4.6.2-1 Unified Communications for Collaboration

The Collaboration standards will continue to mature and converge with enhanced/advanced technologies. The digital convergence will bring about the Unified Storage and Unified Communications that will significantly improve the business process. Text, graphics, applets, streaming media, real-time conference sessions, and other content types will be stored in unified data/message stores. Collaboration Services along with other CES will make use of unified data/message stores. Users will be able to work transparently through a robust grid of communications connectivity through multi-media devices. Security and Bandwidth issues will continue to be improved and resolved as exemplified by DoD PKI and GIG Bandwidth Expansion (BE). The Collaboration service's integration with Translingual Services will provide effective communications among DoD/Allied organizations and commercial enterprises around the globe, and overcome cultural/language barriers.

4.7 Storage

Storage - Basic Capabilities

- Shared Storage Capacity
- Enterprise Storage Architecture
- Storage Capacity on Demand
- Storage Management

The Task-Post-Process-Use (TPPU) paradigm will push today's storage limitations beyond their current capabilities. Supporting this operational model will require the ability to quickly and securely access tremendous amounts of data and information from any location within the GIG. To be successful, DoD must transform itself into what the Gartner Group calls a *zero latency* organization that has the ability to quickly exchange information across technical and organizational boundaries in order to gain an advantage. (Gartner 2001) Supporting this type of dynamic environment and operational paradigm means that DOD must move from the current platform-centric data and information storage and retrieval model to one where enterprise-class data storage and retrieval centers equipped with state-of-the-art technologies allow for easier access while still protecting the data and information from unauthorized use and access.

Today's platform-centric model where data and information is typically co-located with the information processing platform itself must to shift to one where data is made widely available to a variety of processing platforms supporting different Community Of Interest applications and services that need to access the same data or information. Rather than multiple organizations gathering, manipulating, and maintaining multiple copies of the same data DoD must to shift to a model where authoritative sources of data are established that are widely accessible to any authorized user or service. Once authoritative sources of data are define and published, appropriate content can be stored at the network edge, closer to the end users. This would help reduce network and server bottlenecks that slow down and even terminate delivery of critical data and information to the Warfighter.

Another problem with the way that data and information is stored today is that it is typically hard to access it from outside of the platform or enclave where it is stored. This is complicated by the increasingly widespread implementation of Information Assurance (IA) devices like firewalls and other filtering and access control mechanisms and technologies. It is also complicated by the fact that data and information is typically created for a single community of users. This usually means that the data and information is also accessible only to that community of users. DoD must move to a model where, while data and information may be created for a single community of users, it is also easily accessible to other communities of users. This is not so much a shift in technology as it is a shift in culture and perspective as to how data and information is created and how it is shared.

Although TPPU will make data and information more readily accessible, this must be done within the boundaries of current statutory and regulatory guidelines. Information storage and retrieval architectures and technologies must be able to implement access controls and other protection mechanisms to insure that different categories of data or information are adequately protected. For instance, storage services must be able to limit access to Privacy Act information and of implementing HIPPA security requirements to protect a Service Member's medical records. (HHS 2003)

It should be noted that although it's currently presented as a separate service, Storage services could logically also be presented as a direct subset or service offering within the Application service area given that there is an extremely close, almost unbreakable relationship between data and information storage and current processing platforms and functional applications.

4.7.1 Strategy For Increment I

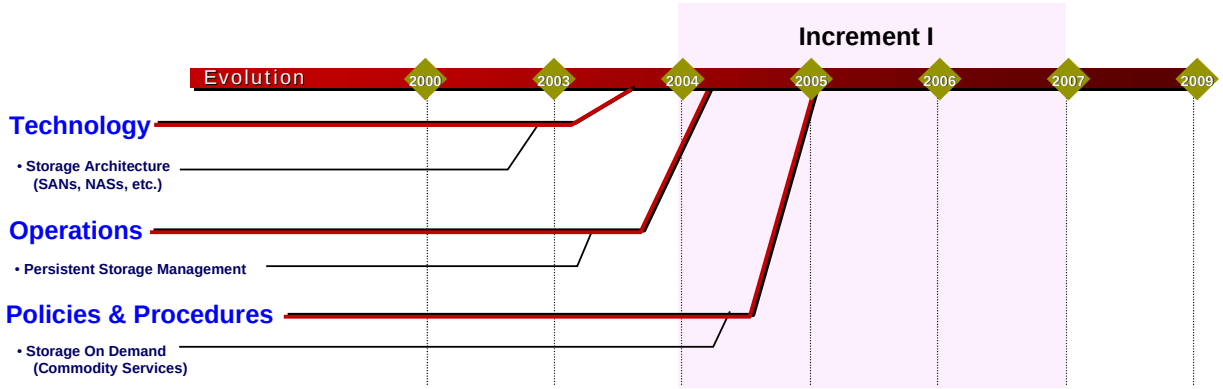


Figure 4.7.1-1 Storage Service Evolution

Technology

The technical strategy for Increment I will focus on moving from the current platform-centric storage model to one based on the wider use of state-of-the-art storage and retrieval technologies and architectures. This will include increased use of Network Attached Storage (NAS) devices and Storage Area Networks (SANs) implemented using various technologies but with a goal in all cases of making data and information more widely and easily accessible to different CoI applications and services. The ultimate goal for Increment I will be to create and foster an environment where data and information storage and retrieval is available on demand.

Operations

In addition to selecting and implementing the right combinations of technologies, there must be an increased emphasis on establishing an operational storage model and architecture that provides for the consistent management and security of persistent storage across the enterprise. Critical to this will be ensuring that the storage service is itself secure and highly available and not subject to any single points of failure.

As already previously noted in paragraph 4.3's discussion of computing capacity, in today's world each individual material or solution developer typically plans for their own storage mechanisms. They plan for certain sizes and capacities of hard drive space or for tape backups or for whatever combination of technologies they feel will meet their specific requirements. The Storage service will move to a new data and information storage and retrieval model where a service or application developer makes their storage and retrieval requirements known to a storage service provider who in turn provides the necessary capacity. An effective and efficient storage service will also be an essential element to addressing back-up and recovery requirements as well as being a critical element of large-scale Continuity Of Operations Planning (COOP) since both of these are very storage intensive operations.

Policies and Procedures

Not only will this approach reduce the cost and complexity of the development process, it should greatly increase the overall efficiency of storage operations because you we will be able to leverage economies of scale and insert new technology on a more consistent basis. Moving to a commodity based storage environment will also support implementing more closely monitored and controlled access controls and other protective mechanisms. And again, rather than each individual material developer having to develop their own access control mechanisms they can make their requirements known to the storage service provider who would then implement them. Being able to consistently apply security policies across the GIG will be absolutely essential in the type of sharing environment envisioned by TPPU.

As with the Application service, one of the primary Increment I objectives of the Storage service would be to develop a Storage On Demand service or capability where storage capability is added at a rate that at least equals the projected requirements to include identified surge requirements. Adopting and implementing the GES Storage service model would also preclude the requirement for every developer to plan and build for a worst case storage capacity scenario by providing highly available and secure Storage on Demand capabilities. Finally, as with other GESs, implementing this kind of enterprise storage capability and fundamentally changing the way that material developers approach the problem of storage will require changing current guidance and policy.

4.7.2 Strategy Beyond Increment I

Since the Storage service is core to the development, testing and deployment of Core Enterprise and Community of Interest applications and services it must be front-loaded into the GES development process. If the Storage service is not developed and deployed early in the overall GES life-cycle, DoD runs the risk of continuing the current approach whereby material developers would continue to develop custom solutions designed to meet their specific set of requirements. Breaking that model requires a fundamental change in how storage requirements are addressed and in how applications and services are developed, deployed, operated and maintained. Beyond Increment I the strategy for the Storage service would be to embark on a continuous process of smart technology insertion and refresh using a controlled process to ensure that a stable, robust, managed, and secure storage infrastructure is established and maintained for the long-term.

4.8 Information Assurance (IA) / Security

Security - Basic Capabilities

- Access management
  - Identity management
  - Authentication
  - Authorization
  - Access enforcement
- Cross-classification connectivity
- Logging and auditing

The Information Assurance / Security (IAS) CESs are a framework and family of services that provide a foundation to implement uniform, consistent, and effective security. The IAS CESs contribute to, but are not sufficient to ensure the security of each service. IAS CESs are invoked as needed by service providers and users to satisfy business and policy requirements and reduce costs.

The service model in general has significant security considerations. While a group of core services can provide a common, reliable and benign operational environment, security-related services provide Information Assurance (IA) capabilities that are commonly required across the enterprise. These IA services can be best provided by the enterprise to: reduce costs; increase implementation consistency, increase the security of assets, service providers and service consumers; make possible enterprise-wide capabilities; and consistently manage enterprise security. In the service model, security capability benefits can include:

- More effective leveraging of specialized expertise
- Continually evolving, best-of-breed security capabilities abstracted from application services implementations
- Fully leveraging *enterprise* business processes, such as the recognition that a person has left the DoD or is for some other reason no longer to be trusted
- Fast, world-wide results of administrative actions

Net-centric enterprise services also create new security challenges for service providers and consumers. Services must be designed, developed, fielded and managed to satisfy IA business and policy requirements of consumers, data owners, service providers and environment providers. Service providers benefiting from services operated by other service providers are forced to rely on these other services to contribute to their own ability to promise the reliability and availability of the service they provide. Enterprise service providers must satisfy data owners that their data will be continually adequately managed with controls such as access management and auditing.

The service provider is faced with the challenge that there is a possibility of software-development-related errors or vulnerabilities within service-provider components. Resolution of this issue involves such concepts as quality assurance and such mechanisms as service-specific input validation. Further, while each service provider component and the environment in which it resides may be "secure," care must be taken that undesirable end-to-end characteristics, including vulnerabilities, don't emerge from the composition of services.

4.8.1 Strategy For Increment I

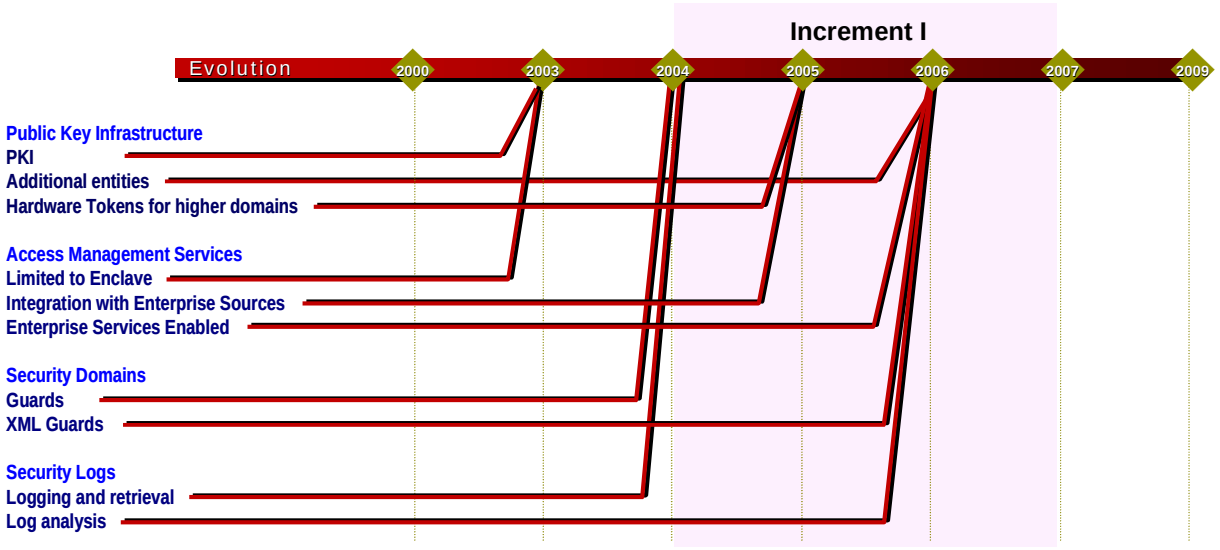


Figure 4.8.1-1 IA/Security Evolution

Access Management

In Increment I, the IAS CESs will provide an enterprise access management service. The access management service will maintain and use identity, roles, privilege, and policy information to aid other services' access authorization decisions by performing the following:

- **Maintaining identity attributes for different types of entities including people, organization, devices, and services.** People may have several different types of identities. Examples are personal, organization, and role-based identities. The identity management component will maintain various identity and authentication attributes. Attributes for individuals might include personnel identifiers, human name, birth date, social security number, digital certificates, and biometric information. The biometric information may include a facial image, fingerprints, or an iris scan and could be used to augment or replace cryptographic authentication. The access management service will maintain appropriate identity attributes for the other entity types.
- **Providing and maintaining enterprise authentication capabilities for all entities**. IAS CESs will include the credential registration, credential status checking and possibly run-time authentication of entities. Public key and biometric technologies are evolving as enterprise authentication credential capabilities. Public key technology also supports message-level confidentiality. It may become possible for the enterprise to provide service-level authentication as a service.
- **Maintaining authorization information for entities.** The authorization information will consist of additional attributes that describe or determine the entity's rights to access services. The use of the authorization attributes will depend on the context and the entity's role in an access request.
- **Access enforcement.** The decision engine that, given information about the identities and authorization attributes of the entities involved in an access request, determines whether the access should be allowed. The decision engine will follow an appropriate access policy to make the access decision. Service providers will be able to establish rules for access to their services.

The access management system will function as if there were a centralized access management service. In practice the access management system may be implemented as a distributed service or a federation of coordinated services, potentially improving performance and avoid single points of failure. In the increment's initial spirals, the access management service may be limited to a local enclave or CoI. Pursuit of multiple versions of the access management will help identify requirements and "best of breed" approaches. The service will evolve in later spirals to expand and integrate the enclaves' services and their data repositories. Efforts in the later spirals will attempt to identify and integrate existing, related data sources and repositories.

Some components of the access management service may have to interact with the Discovery CESs to allow discovery of entities and their various access-related attributes.

Cross-Classification Connectivity

The cross-classification connectivity services, such as guards, will provide enterprise capabilities of selective sharing of information across security boundaries. As a general capability, this is most likely to be able to be provided as an enterprise that permits information to be sent up to domains of higher levels of sensitivity. Enterprise support for messaging can be provided in both directions.

Logging and Audit

Logging services will provide an ability to record security events. Logs of security events are useful for determining that systems are not being abused or violated and to hold individuals accountable for their actions. Initially, the IAS CESs will provide basic capabilities to store and retrieve log information and, in later spirals, will evolve to provide automated analyses of the logs. Security services and tools may be configured to automatically scan logs to detect user or service use anomalies and notify the system and security manager. For example, the automated analysis may correlate seemingly diverse, disparate events that are in reality the product of a coordinated network attack. The availability of logs make possible business-level audit of activities. Effective audit can provide a significant deterrent from insider attacks. Time stamping or notarization may also be provided as an enterprise service. Through authentication, audit, and time stamping services, IAS CESs can reduce costs and increase effectiveness of business entities that have need of "non-repudiation" capabilities.

4.8.2 Strategy Beyond Increment I

Increment II may provide Digital Rights Management (DRM) as an enterprise-wide capability. This commercial capability is rapidly evolving and promises to fundamentally change DoD's ability to manage the confidentiality of sensitive information.

The remainder of the emphasis for Increment II and beyond will be to adapt and extend the IAS CESs to support the use of mobile and wireless devices and to ensure that the services can scale to an environment where virtually all communications occur on the net (service anywhere / anytime).

GES allow producers and consumers to access and utilize the data. As the network becomes the common communication environment for all systems and devices from command and control sensors as well as control environmental and power systems in buildings, devices may likely become the predominant entity rather than users/individuals. By the time Increment II is fielded, the number of devices needed to be managed and supported may have grown by an order of magnitude.

4.9 User Assistance

User Assistance - Basic Capabilities

- Section 508 accessibility validation tools
- Smart agents - content monitoring

The User Assistance (UA) services have the common characteristic of being directly end-user facing or enabling end-user activities. Their purpose is to be automated "helper" capabilities for potential service or data consumers that reduce the effort required to perform manpower intensive tasks.

The UA CESs use a variety of emerging technologies in Increment I. For example, Section 508 validation allows service providers across the net to efficiently provide accessible services and content to end-users. Smart agent technology allows end-users to monitor large quantities of ever-changing content with configurable alert or reporting mechanisms.

4.9.1 Strategy For Increment I

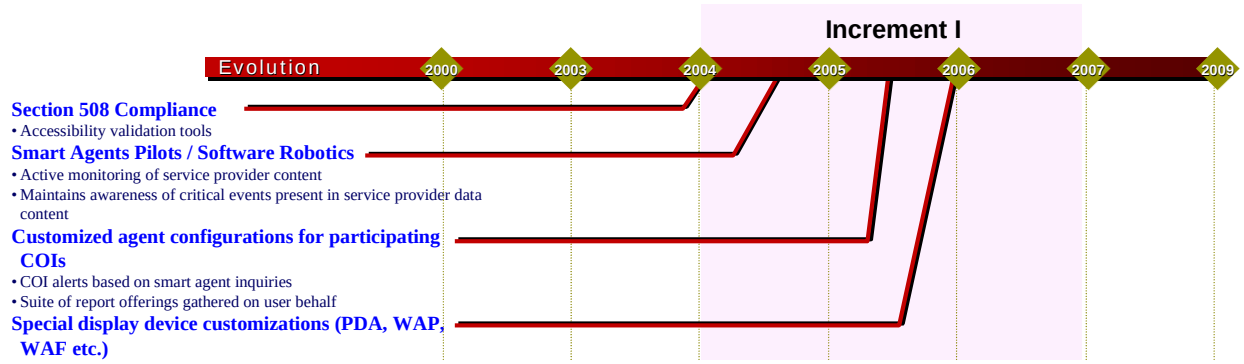


Figure 4.9.1-1 User Assistance Evolution

Section 508 Compliance

In 1998, Congress amended the Rehabilitation Act to require Federal agencies to make their electronic and information technology accessible to people with disabilities. Section 508 was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities, and to encourage development of technologies that will help achieve these goals. (CITA 2003) A key portion of the UA CES is to provide Section 508 support.

Section 508 compliance frequently requires human intervention to resolve content, perception, and tagging issues that only human cognition and judgement calls can currently solve. For example, 508 compliant Web pages require that images in the page have a description. The text appears in most browsers when the mouse crosses over the image. The image description is based on the content of image in the context of the Web page. Unfortunately, these descriptions are not items that can be automatically produced by today's software. However, today's tools can still be a great aid to the CoI attempting to produce 508 compliant content on the net. Currently, there are several commercial tools that support the validation of Section 508 accessibility rules in graphical user interfaces such as application screens in Web browsers. While human intervention is still required for several cognitive activities, the tools save substantial resources. The first step in the user assistance strategy is to make Section 508 validation capabilities available on the WANs where service providers reside shall be developed. Currently, such tools are available on the public Internet under Federal initiatives.

Smart Agents Pilots / Software Robotics

While services in the Discovery CES will provide the capability to find data providers with content on the net, the UA CES adds the capability for end-users to actively monitor service provider content

through the use smart agents technology. For example, a user can discover that MSNBC is a provider of "raw" news articles, but being alerted when a terrorism event is written about, within that collection, is an additional capability. Smart agent technology allows the user to maintain awareness of critical events present in multiple sources of service provider data content. Traditionally, this would be a manually intensive and repetitive task.

Smart agent technology pilots will be initiated that investigate the following strategic capabilities on behalf of end-users:

- Customized agent configurations for participating CoIs - ontology specific CoI alert triggers based on smart agent inquiries
- Suites of report offerings gathered on user behalf
- Special agent display device customizations (PDA, WAP, WAF etc.)

The intent of this capability is not to do work that is correctly in the CoI role, but to provide common tools that enable and further CoI content management. Therefore, when these tools are in place at an enterprise level, end-users can have common expectations about agent capabilities regardless of the CoI(s) that they belong to.

4.9.2 Strategy Beyond Increment I

The UA core services will continue to rapidly evolve after the Increment I time period. Ongoing commercial and DARPA-related research will be routinely investigated to identify any candidates for potential pilot projects or technology refreshments beyond Increment I. Commercial progress in the fields of smart agents and user assistance is rapid and will require adjustments in the planning cycle.

5 Summary

5.1 Strategic Challenges

Implementation of the capabilities described in this strategy will be subject to a wide set of technical, operational, programmatic, and cultural challenges, most of which will be mitigated through more detailed program planning and governance. This section of the strategy will focus on identifying those critical strategic challenges inherent in adopting a transformational shift of this magnitude, accomplished under a new set of acquisition guidance, and based on a technical foundation that requires a fundamental shift from systems-based to services-based constructs.

DoD Transformation objectives have thus far been articulated through a Net-Centric Data Management Strategy. This sets the appropriate focus on end user capability and value to the warfighter. The comprehensive, integrated approach necessary for successful transformation will also require a much broader set of strategic guidance that will define the ground-breaking new approaches needed to transform the technical, operational, and business approaches associated with the shift to a services-based environment. To this end, a series of strategic white papers is recommended to address the following challenges:

New Concepts and Roles	Description
Service Oriented Architectures	Existing DoD architectural constructs do not provide a framework and taxonomy for defining the delivery of services. New approaches for defining Service Oriented Architectures are emerging, and need to be adapted or adopted for use by GES, prior to the definition of Increment I architecture.
Standards and Compliance	Current notions of compliance focus on adherence to a set of specified standards and interfaces at build time and run time. A shift toward composable services will require a shift toward a build time/compose time/deploy time/ run time paradigm that alters notions of when compliance is achieved, as well as changes in the ideas of what constitutes compliance..
Service Testing	Traditional DT/OT approaches may require extensive tailoring for alignment with incremental evolutionary spirals. Further, application of traditional DT/OT to the fielding of composable services will not adequately identify risks to the environment at large as new services are declared operational. Staging environments, technical and security risk reduction, and load testing of large-scale enterprise capabilities need consideration.
Service Provider Role	Assured service delivery will be based on coordinated cooperation across DoD entities to ensure that specific service level agreements are met consistently. A business construct defining the roles of a service provider, and requiring service providers to set minimum standards for service delivery, will be necessary to achieve guaranteed service delivery across the enterprise.

Implementing Strategies	Description
Development and Fielding Strategy	The life cycle for services differs significantly from the traditional systems life cycle. Service creation, service delivery, service management, and service retirement will need to be strictly defined to guide consistency across the enterprise. Likewise, the governance approach for determining service advancement through the life cycle must also be determined.
Operations and Management Strategy	To the extent possible, existing hosting environments must be leveraged to accommodate emerging capabilities. If this holds true, then existing centers will require significant changes to assure that security, management, and distribution capabilities will be adequately supported. The extent to which hosting environments for core enterprise services must be interoperable with and supported by environments within the CoIs requires early definition.
Increment I Investment Strategy	Early CES capability will be based on evolution from existing Program of Record capabilities, fundamentally based on COTS. However, application of new technology will also require strategic expenditure of R&D funds to accelerate the most needed and most promising emerging technologies.
Transition Strategies	Transition strategies addressing transition of Program of Record capabilities into the CES environment will be critical to understanding where and how capabilities will emerge, and where gaps will be encountered. Transition strategies for users of CES will also be critical for understanding the timing of the emergence of CES capabilities to meet end user needs and expectations.

5.2 Conclusion

Achieving net-centric transformation will require the active participation of all DoD Components under the guidance of the net-centric governance process. The further definition and synchronization of transformational capabilities and services will be achieved in an evolutionary fashion, with continual refinement and communication of strategies and approaches throughout the DoD constituency. This Increment I strategy will be revisited as required to meet overall DoD objectives.

Appendix A: List of References

ASD NII,. (May 2003), "*Global Information Grid Enterprise Services (GIG ES) Implementation*"

Center for IT Accommodation (CITA), Office of Governmentwide Policy, U.S. General Services Administration. (May 2003) "*508 Law*" [On-line]. Available: http://www.section508.gov/index.cfm?FuseAction=Content&ID=3

Defense Information Systems Agency (DISA), (May 5, 2003), "*Global Information Grid (GIG) Enterprise Services (GES) Analysis Of Alternatives (AoA) Study Plan*"

Department of Health and Human Services (HHS), (May 2003) "*Administrative Simplification in the Health Care Industry*" [On-line]. Available: http://aspe.os.dhhs.gov/admnsimp

Department of Defense (DoD) Chief Information Officer (CIO), (August 24, 2000), "*Guidance & Policy Memorandum No. 10-8460 – Network Operations*"

Deputy Secretary of Defense, (December 24, 2002) "*Net-Centric Business Transformation and e Government*"

Defense Information Systems Agency (DISA), (October 2, 2002) "*Net-Centric Enterprise Services (NCES) Definition Study*"

Defense Information Systems Agency (DISA), (June 2002), "*Transformation Roadmap*"

Ford, W., P. Hallam-Baker, B. Fox, B. Dillaway, B. LaMacchia, J. Epstein, and J. Lapp. (March 30, 2001). "*XML Key Management Specification (XKMS)"*. World Wide Web Consortium (W3C). W3C Note. [On-line] Available: http://www.w3.org/TR/xkms.

Gartner Group, (May 2001), "*An Approach to Building a Business Case for Zero-Latency – Prepared for Compaq Telecom*"

Godik, S., T. Moses. (February 18, 2003), "*eXtensible Access Control Markup Language (XACML)"*, Version 1.0. Organization for the Advancement of Structured Information Standards (OASIS). OASIS Standard,. [On-line] Available: http://www.oasis-open.org/committees/xacml/repository/

Hallam-Baker P., E. Maler. (November 5, 2002), "*Security Assertion Markup Language (SAML)"*. Organization for the Advancement of Structured Information Standards (OASIS). OASIS Standard, [On-line] Available: http://www.oasis-open.org/committees/security/docs/

Indiana Department of Education (IDOE), (April 1996), "*What Economics Is About*"

Maedche A., Motik B., Stojanovic L., Studer R. and Volz R. in IEEE Intelligent Systems, Volume 18, Number 2, pp. 26-33, March/April 2003 "*Ontologies for Enterprise Knowledge Management*" [On-line]. http://kaon.semanticweb.org/docus/ieee-is-maedcheetal.pdf

MCEB NetOps Panel, (November 12, 2002), "*Joint NetOps CONOPS (Draft Version 3.0)"*

Stenbit, J. (April 2, 2002) "*OASD(C3I) TPPU Concept for Network Centric Operations*"

TeleManagement Forum, (2001), "*System Integration Map - Deliverable 1: Concepts and Principles*"

TINA Consortium, Kristiansen L. (ed.), (June 1997), "*TINA Service Architecture Version 5.0.*"

TINA Consortium, (May 1997), "*TINA Business Model and Reference Points, Version 4.0*"

U.S. Joint Forces Command, (August 30, 2001), "*Capstone Requirements Document (CRD) Global Information Grid (GIG) JROCM 134-01*"

Appendix B: Acronyms

ACID	Atomicity, Consistency, Isolation, and Durability
ACTDs	Advanced Concept Technology Demonstrations
API	Application Programming Interface
ASP	Application Service Provider
AT&L	Acquisition, Technology, and Logistics
AoA	Analysis of Alternatives
ASD/NII	Assistant Secretary of Defense for Networks and Information Integration
B2B	Business-to-Business
BPM	Business Process Management
CAN	Campus Area Networks
C^2	Command and Control
CC/S/A	Combatant Commands, Services and Agencies
CM	Configuration Management
CND	Computer Network Defense
CIO	Chief Information Officer
COE	Common Operating Environment
CO1	Community of Interest
C3I	Control, Communications, and Intelligence
CES	Core Enterprise Service
CONUS	Continental United States
COOP	Continuity of Operations
COTS	Commercial Of The Shelf
DARPA	Defense Advanced Research Projects Agency
DEBX	Defense EB Exchange
DISN	Defense Information System Network
DISA	Defense Information Systems Agency
DITSCAP	Defense Information Technology Security and Accreditation Program
DoD	Department Of Defense
DT/OT	Diagnostic Test / Operational Test
UDF	User Defined Format
EA	Executive Agent
EBXML	Electronic Business XML
EDI	Electronic Data Interchange
ERP	Enterprise Resource Planning
ESM-NetOps	Enterprise Service Management–Network Operations
ESM	Enterprise Systems Management
FCAPS	Fault, Configuration, Accounting, Performance and Security Management
FY	Fiscal Year
GDS	Global Directory Services
GENSER	General Service
GES	GIG Enterprise Services
GIG	Global Information Grid
GES	(GIG) Enterprise Services
GOTS	Government Off The Shelf
GUI	Graphical User Interface
HGS	High Grade Service
HIPPA	Health Insurance Portability and Accountability Act

HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IA	Information Assurance
IAS	Information Assurance/Security
IAVA	Information Assurance Vulnerability Alerts
IC	Intelligence Community
IDM	Information Dissemination Management
IEEE	Institute of Electrical and Electronics Engineers
IM	Instant Messaging
IP	Internet Protocol
IS	Interface Specification
IT	Information Technology
JROC	Joint Requirements Oversight Council
JTF	Joint Task Force
JWICS	Joint Worldwide Intelligence Communications System
KMI	Key Management Infrastructure
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAN	Metropolitan Area Networks
MCU	Multipoint Control Unit
MGS	Medium Grade services
MOE	Model Operating Environment
NAS	Network Attached Storage
NCES	Net-Centric Enterprise Services
NCW	Network Centric Warfare
NII	National Information Infrastructure
NIPRNET	Non-Secure Internet Protocol Router Network
NNTP	Network News Transport Protocol
O&M	Operated and Maintained
OMG	Object Management Group
OAN	Operational Area networks
OCONUS	Outside the Continental United States
QOS	Optional Quality of Service
PC	Personal Computer
PDA	Personal Digital Assistants
PKI	Public Key Infrastructure
PM	Program Manager
POR	Programs of Record
QoS	Quality of Service
R&D	Research and Development
RTE	Real Time Enterprise
S&NM	Systems and Network Management
SAL	Service Level Agreements
SAML	Security Assertion Markup Language
SAN	Storage Area Networks
SAP	Simplified Acquisition Points
SCI	Sensitive Compartmented Information (SCI)
SIGINT	Signals Intelligence
SIPRNET	Secret Internet Protocol Router Network

SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
SQL	Structure Query Language
TCP/IP	Transmission Control Protocol/ Internet Protocol
TINA	Telecommunications Information Networking Architecture
TPPU	Task, Post, Process, Use
TPED	Task, Process, Exploit, Disseminate
UDDI	Universal Description, Discovery and Integration
UDF	User Defined Formats
VPN	Virtual Private Networks
VTC	Video Teleconference
WAF	Web Application Framework
WAP	Wireless Application Protocol
WAN	Wide Area Networks
XACML	Extensible Access Control Markup Language
XKMS	XML Key Management Specification
XML	Extensible Markup Language
ACTDs	Advanced Concept Technology Demonstrations
AT&L	Acquisition, Technology, and Logistics
AoA	Analysis of Alternatives
B2B	Business-to-Business
CAN	Campus Area Networks
C^2	Command and Control
COE	Common Operating Environment
CO1	Community of Interest
C3I	Control, Communications, and Intelligence
CES	Core Enterprise Service
COOP	Continuity of Operations
COTS	Customer Of The Shelf
DEBX	Defense EB Exchange
DISN	Defense Information System Network
DISA	Defense Information Systems Agency
UDF	User Defined Formats
DoD	Department of Defense
EDI	Electronic Data Interchange
ESM-NetOps	Enterprise Service Management–Network Operations
ESM	Enterprise Systems Management
EA	Executive Agent
FCAPS	Fault, Configuration, Accounting, Performance and Security Management
FY	Fiscal Year
GENSER	General Service
GES	GIG Enterprise Services
GIG	Global Information Grid
GUI	Graphical User Interface
IC	Intelligence Community
IMAP	Internet Message Access Protocol
IS	Interface Specification
JROC	Joint Requirements Oversight Council
JTF	Joint Task Force

LAN	Local Area Network
MAN	Metropolitan Area Networks
NCES	Net-Centric Enterprise Services
NCW	Network Centric Warfare
OMG	Object Management Group
OAN	Operational Area networks
QOS	Optional Quality of Service
PBX	Private Branch Exchange
PDA	Personal Digital Assistants
PM	Program Manager
PKI	Public Key Infrastructure
POP	Post Office Protocol
QOS	Quality Of Service
R&D	Research and Development
SAL	Service Level Agreements
SCI	Sensitive Compartmented Information (SCI)
SIGINT	Signals Intelligence
TAP	Tele-locator Alphanumeric Protocol
TINA	Telecommunications Information Networking Architecture
TPPU	Task, Post, Process, Use
TPED	Task, Process, Exploit, Disseminate
VPIN	Voice Profile of Internet Mail
VPN	Virtual Private Networks
VTC	Video Teleconference
WAN	Wide Area Networks
WAP	Wireless Application Protocol
WCTP	Wireless Communication Transfer Protocol
XML	Extensible Markup Language

1

Appendix C: Glossary

Application Programming Interface (API) - A programmer's guide that describes the software libraries and services, and how to write software modules that interface with and use the services. (I&RTS, V2.0, OCT 95] In a net-centric paradigm, the services invoked may reside across the network at another platform.

Application Service – The set of service offerings that provide a protected operational environment consisting of common hardware platforms, operating systems, and applications that will be used to host CES and CoI services.

Battlespace - The environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, sea, space, and the included enemy and friendly forces; facilities; weather; terrain; the electromagnetic spectrum; and the information environment within the operational areas and areas of interest (Joint Pub 1-02).

Collaboration - Near real-time human interaction supported by connectivity configurations while preserving security of multiple systems and sources across geographically dispersed sites and organizations. Examples include Instant Messaging (IM), shared whiteboards, and video conferencing. Provides timely, secure, and ubiquitous edge-user access, from any compliant platform on the net-centric enterprise infrastructure.

Commercial-Off-The-Shelf (COTS) - Refers to an item of hardware or software that has been produced by a commercial organization and is available for general purchase.

Common Operating Environment (COE) - The COE is an integrated software infrastructure, which facilitates the migration and implementation of functional mission applications and integrated databases across information systems. The DII COE provides architecture principles, guidelines, and methodologies that assist in the development of mission application software by capitalizing on a thorough, cohesive set of infrastructure support services. (DII Master Plan, V5.0, NOV 1996)

Configuration Management - A discipline applying technical and administrative direction and surveillance to: (1) identify and document the functional and physical characteristics of a configuration item; (2) control changes to those characteristics; and (3) record and report changes to processing and implementation status. (Joint Pub 1-02)

Core Enterprise Services (CESs) - A collection of networked capabilities that enable DoD service providers. The CESs provide and manage the underlying capabilities to deliver content and value to end-users, and are currently binned into nine groups as defined in Section 4 of this document.

Defense Information Infrastructure - The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving Department of Defense (DOD) local, national, and worldwide information needs. The defense information infrastructure connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DoD information. (Joint Pub 1-02).

Discovery - Discovery includes knowledge and data resource detection, and identification by consumers.

End-user - The final human user of information on the net. The user on the "edge" of the net. Not a system to system or B2B consumer of a service.

Enterprise service - A service intended for enterprise-wide consumption. Please see "service".

Enterprise Service Management (ESM) Service – The set of service offerings that provide the suite of operational processes, procedures and technical capabilities needed to ensure: that GIG Enterprise Services (GES) are up and running, accessible and available to users, protected and secure; that they are properly

provisioned and operating and performing within agreed upon parameters; that problems are proactively detected, isolated and resolved with the minimum impact to the user; and that managers at all levels have access to a shared IT situational awareness.

GIG Enterprise Services (GES) - A collection of net-based capabilities for use in the DoD enterprise. The GES is composed of the networks, the core services, and the community services combined.

Global Information Grid (GIG) - The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to Warfighters, policy makers and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996 (CJCSI 6212.01B).

Information Assurance (IA) - Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP 1-02)

Loosely coupled - Loosely coupled services, even if they use incompatible system technologies, can be joined together on demand to create composite services. Participants must establish a shared framework to ensure messages retain a consistent meaning across participating services. (louslycoupled.com)

Mediation- A third-party capability that acts as a facilitator to assist in communication between two end-points. The end-points can be systems, applications, or users. The mediation capability can perform tasks such as assured delivery, rapid delivery, or translation of content, and auditability of interactions between the parties. Mediation is derived from concepts in the software field of Enterprise Application Integration (EAI).

Messaging - Provides the ability to exchange information securely among users or applications on the net-centric enterprise infrastructure (i.e. E-mail, DoD-unique message formats, secure instant messaging, notification and awareness services (Publish/Subscribe), and alerts. The creation, storage, exchange, and management of text, images, voice, telex, fax, e-mail, paging, and Electronic Data Interchange (EDI) over a net.

Net-centric – A networked collection of capabilities that empower the edge user to pull the information they require, from any available source, with minimal latency, to support the mission at hand.

Net-Centric Enterprise Services (NCES) - A DISA program to implement key enabling capabilities for a net-centric enterpise. NCES will provide a common set of interoperable information capabilities in the Global Information Grid (GIG) to access, collect, process, store, disseminate, and manage information on demand for warfighters, policy makers, and support organizations.

Network Centric Warfare - An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. Network centric warfare translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.

NetOps - An integrated approach to accomplishing the three interdependent functional areas —System and Network Management (S&NM) [also referred to as NSM or ESM], Information Assurance/Computer Network Defense (IA/CND), and Information Dissemination Management (IDM). NetOps consists of the organizations, processes, and functionalities required to plan, administer, and monitor the GIG infrastructure and information dissemination in support of operations and responding to threats, outages, and other operational impacts. (Joint Concept of Operations for Global Information Grid NetOps Version 3.0 dated May 30, 2003)

Publish/Subscribe - A method of interacting between a content producer and a consumer. Channels are created which hold dynamically created event content. Consumers subscribe to the channels to have access to the content. Business rules that cross events in multiple channels can derive rich and complex relationships in information.

Producer - In the consumer/producer pair, the producer creates and offers something of value to the consumer. Synonymous with a service provider in the context of this paper.

Service - A service is a software system whose public interfaces and bindings are defined and described. Its definition can be discovered by other software systems. These systems may then interact with the Web service in a manner prescribed by its definition, using structured messages conveyed by Internet protocols. (Definition borrows from WC3)

Service Level Agreement (SLA) - An agreement between the provider of a service and the consumers of a service. The agreement can outline service attributes such as monitoring and measurement mechanisms, performance metrics, compliance, remedies, and termination.

Service Oriented Architecture (SOA) - A service-oriented architecture is essentially a collection of services. These services communicate with each other. The communication can involve either simple data passing or it could involve two or more services coordinating some activity. Some means of connecting services to each other is needed. (service-architecture.com)

Service Provider - An organization that implements and operates a service on the net. An effective provider must continually strive to understand the audience for a service and live up to the promised service levels. A service provider's product is the service on the net that they make possible.

Storage Service – The set of service offerings that provide devices and networks that are designed and built primarily for the persistent storage, protection, and retrieval of data and information between CES and CoI services and applications, between inter-connected computer systems, and between computer systems and end-users.

Unified Messaging - Unified messaging is the integration of several different communications media, such that users will be able to retrieve and send voice, fax, and e-mail messages from a single interface, whether it be a wireline phone, wireless phone, PC, or Internet-enabled PC. (iec.org)