

Department of Defense Net-Centric Services Strategy

Strategy for a Net-Centric, Service Oriented DoD Enterprise



May 4, 2007

**Department of Defense
Chief Information Officer
The Pentagon—Washington, D.C.**

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 04 MAY 2007		2. REPORT TYPE		3. DATES COVERED 00-00-2007 to 00-00-2007	
4. TITLE AND SUBTITLE Strategy for a Net-Centric, Service Oriented DoD Enterprise				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Department of Defense, Chief Information Officer, The Pentagon, Washington, DC				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

FOREWORD


The Internet has facilitated an e-commerce explosion in the private sector through the ready access of information and business services; it has also helped companies lower costs across supply and demand chains, dramatically improve customer service, and redefine business relationships. The Department of Defense (DoD) Net-Centric Services Strategy (NCSS) reflects the DoD's recognition that this service oriented approach can result in an explosion of capabilities for our warfighters and decision makers, thereby increasing operational effectiveness. A service oriented approach can accelerate the DoD's ongoing effort to achieve net-centric operations by ensuring that our warfighters receive the right information, from trusted and accurate sources, when and where it is needed.

The DoD NCSS builds upon the DoD Net-Centric Data Strategy's (May 2003) goals of making data assets visible, accessible, and understandable. This strategy establishes services as the preferred means by which data producers and capability providers can make their data assets and capabilities available across the DoD and beyond. It also establishes services as the preferred means by which consumers can access and use these data assets and capabilities.

The DoD's vision is to establish a Net-Centric Environment (NCE) that increasingly leverages shared services and Service Oriented Architecture (SOA) that are:

- Supported by the required use of a single set of common standards, rules, and shared secure infrastructure provided by the Enterprise Information Environment Mission Area (EIEMA);
- Populated with appropriately secure mission and business services provided and used by each Mission Area;
- Governed by a cross-Mission Area board, which is chaired by the DoD Chief Information Officer (CIO);
- Managed by Global Information Grid (GIG) NetOps.

When this vision is achieved, all members of the DoD will realize significant benefits. A common infrastructure enables force capabilities to be readily networked in support of joint warfighting and operations. Interoperability of capabilities is improved when Military Services, Agencies, and mission partners create reusable "building blocks" through the use of services. The coordinated management of this environment under GIG NetOps provides the necessary situational awareness for joint forces to use the capabilities that are available. The DoD's commitment to govern this evolution will greatly improve the ability to respond to evolving operations and missions.



John G. Grimes
Assistant Secretary of Defense for
Networks and Information Integration
DoD Chief Information Officer

Table of Contents

1	Purpose	1
2	Introduction	1
2.1	DoD Net-Centric Services Vision	2
2.2	Illustrating the Benefits of Services and SOA	3
	The Current Environment	3
	Evolving Towards Services and SOA	4
3	Net-Centric Services Strategy Goals	5
3.1	GOAL: Provide Services	6
	Provide Mission and Business Services	6
	Provide Core Enterprise Services (CES)	6
	Make Services Visible	6
	Make Services Accessible	7
	Make Services Understandable	7
3.2	GOAL: Use Services	7
	Use Services as a Common Practice	7
	Use CES	8
3.3	GOAL: Govern the Infrastructure and Services	8
	Establish Appropriate Governance Forums	9
	Enable Services to be Trusted	9
	Integrate Service and SOA Enablers into Decision Support and Portfolio Management Processes	9
3.4	GOAL: Monitor and Manage Services via GIG NetOps	9
4	Next Steps	10
5	Conclusion	11
6	Appendix A. Definitions	12
	Appendix B. References	14

Table of Figures

Figure 1 Business Processes and Services 2
Figure 2 Users Look Only to Known Systems for Data and Functionality 4
Figure 3 Populating the NCE with Services 4
Figure 4 Users Look to the NCE for Information and Capabilities 5

Listing of Tables

Table 1 Net-Centric Services Strategy Goals 6
Table 2 Key Actions 10

1 Purpose

This document describes the Department of Defense's (DoD's) vision for establishing a Net-Centric Environment (NCE) that increasingly leverages shared services and Service Oriented Architecture (SOA). The DoD's NCE is a framework for human and technical connectivity and interoperability that allows DoD users and mission partners to share and protect information and to make informed decisions. The NCE consists of numerous mission and business services and common and shared infrastructure services. This strategy is applicable to DoD's Warfighting, Business, DoD Intelligence, and Enterprise Information Environment (EIE) Mission Areas and Joint Capability Portfolios.

The Net-Centric Services Strategy (NCSS) expands upon the DoD Net-Centric Data Strategy (May 2003) by connecting services to the Data Strategy goals. The NCSS is consistent with other DoD net-centric strategies and guidance. Separate DoD issuances will be provided to address NCSS implementation details and specific technical guidance.

2 Introduction

The DoD's March 2005 National Defense Strategy restated its commitment to achieving net-centric operations. The foundation for net-centric operations is the ability for users to obtain the required information and applications when and where they are needed.

As existing threats facing the DoD evolve and as new threats begin to emerge, a new level of responsiveness and agility is required from our forces. The DoD cannot transform its operations to support a net-centric force by merely maintaining and expanding the status quo. Patching stovepipes together is a temporary solution that leads to a fragile environment, which will eventually crumble under the high demands and unpredictable needs of the users. The current DoD network consists of information silos that cannot communicate with each other unless they are pre-wired to do so. In addition, these silos cannot scale to accommodate the levels of interaction that will exist. The DoD's current stovepiped information environment must shift to a more robust and agile information environment that can support and enable net-centric operations.

Achieving the commitments in the National Defense Strategy requires a fundamental change in the way Information Technology (IT) is provided and managed by the DoD. Historically, IT resources and software-based capabilities have been acquired and managed as stand-alone systems rather than as integral parts of a net-centric capability. System-to-system connections are defined, engineered, and implemented one pair at a time. This approach focused on system or platform capabilities rather than on mission capabilities. The result is multiple overlapping implementations, limited ability to share information, and a rigid set of capabilities that are unresponsive to the warfighter's evolving needs.

The commercial world's approach to resolving this problem has been to define business processes as workflows. These workflows consist of specific business functions that are supported by the delivery of software-based services over networks. These software-based services deliver reusable business functionality as standardized building blocks on an enterprise network. Figure 1 shows a simplified workflow for a business process (i.e., inventory

management) in the DoD. The function, “Check Forward Supply” is implemented using software building blocks or services (e.g., a Get Inventory Count service) and provides a distinct element of functionality that can be used in other processes by Military Services, Agencies, Commands, or mission partners. When a new mission capability is required (e.g., needing a new business process for logistics planning for a mission planning application), the Get Inventory Count building block can be quickly used to respond to this new or changing mission need. This approach lies at the core of an SOA.

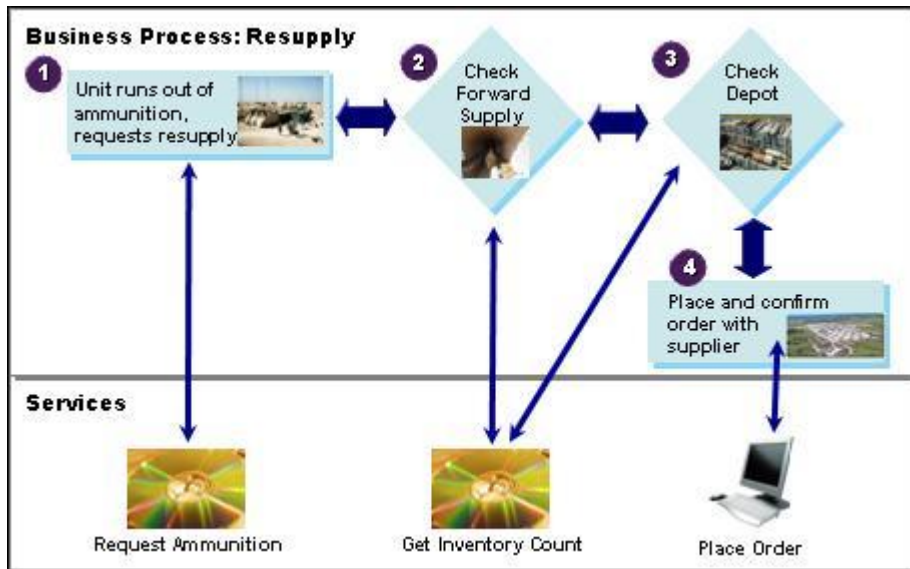


Figure 1 Business Processes and Services

SOA is a way of describing an environment in terms of shared mission and business functions and the services that enable them. With SOA, the DoD must establish and enforce how the service building blocks will be made available, secured, operated, and used by the enterprise. Using the resulting building blocks will facilitate interoperability and joint operations, provide agility, and improve information sharing.

2.1 DoD Net-Centric Services Vision

The existing networks and systems that make up the GIG provide a wide range of information and functional capabilities within each of the Mission Areas. As the Department transforms towards net-centric operations, the DoD NCE will increasingly leverage shared services and Service Oriented Architectures that are:

- Supported by the required use of a single set of standards, rules, and a common, shared secure infrastructure provided by the Enterprise Information Environment Mission Area (EIEMA);
- Populated with appropriately secure mission and business services provided and used by each Mission Area;
- Governed by a cross-Mission Area board, chaired by the DoD Chief Information Officer (CIO);
- Managed by Global Information Grid (GIG) NetOps.

As the vision is achieved, operational effectiveness is improved. A common infrastructure enables force capabilities to be readily networked in support of joint warfighting. When Military Services, Agencies, and mission partners create “building blocks” from their capabilities through the use of services, interoperability of capabilities is improved. Management of this environment in a coordinated fashion under GIG NetOps provides the situational awareness for joint forces to know of and use the capabilities that are available regardless of which Military Service, Agency, or mission partner provided the capability.

Capability providers also benefit from the DoD achieving this vision because -

- Services provide an improved, standards-based approach to achieve information sharing *and*
- Services increase the capability provider’s agility through cost and resource-effective reuse of capabilities.

These benefits are the result of carefully designed services, functioning as the building blocks for key elements of mission or business functionality. Ready accessibility to these services improves user access to new sources of information. Additionally, as previously shown in Figure 1, any capability provider can build a new application using an existing service rather than recreating similar functionality. When capability providers can discover existing capabilities offered as services, they can significantly reduce the time and cost to field a new capability and gain improved interoperability “out of the box”. By using these building blocks, the DoD can quickly adapt to accommodate the warfighters’ changing mission needs.

2.2 Illustrating the Benefits of Services and SOA

Information and functional capabilities provided as services in the NCE will change the way the DoD fights wars and conducts its peacetime business. An NCE that is rich with services does more than effect a technology change; it also changes the ways in which people execute their missions and fulfill their responsibilities.

The Current Environment

Currently users (i.e., warfighters, business users, and developers) typically look only to known systems where access and privileges have been pre-established to fulfill the majority of their information needs and to execute aspects of their missions. This pre-planning has advantages and will continue to be a major element of how the DoD operates. For example, users can quickly access information when they know which system to use and how to use it. However, pre-planning can limit options when a user is faced with operational needs that are different than anticipated. Figure 2 illustrates the limitation of stovepiped environments for both the warfighter and analyst, and the capability developer. Many users use a specific system (e.g., System 1) to conduct their mission. They have been trained on that system and are very familiar with the data and capabilities. However, in joint operations, they frequently find that they need information or functionality to conduct their mission that is not available in their known systems. The users are unaware of the existence of another system (e.g., System 2), or they are unable to access that system. Likewise, the developers that build capabilities are often unaware of the functionality (or “building blocks”) provided by other systems or those other systems may be built such that their functionality cannot be used by another system. The ability to quickly find and use new sources of information and functionality is limited in today’s stovepiped environment.

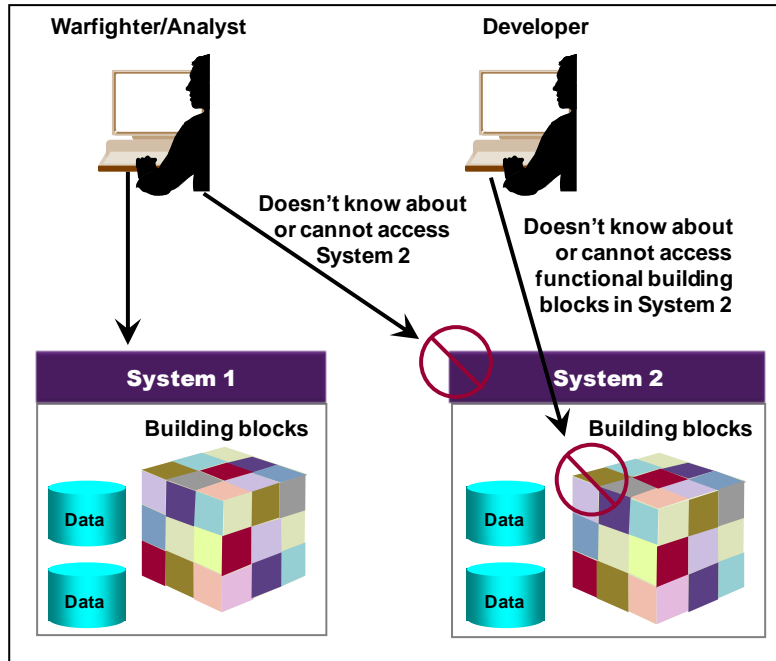


Figure 2 Users Look Only to Known Systems for Data and Functionality

Evolving Towards Services and SOA

As illustrated in Figure 2, DoD needs to improve the way information and functional capabilities are shared. When fielding new or enhanced capabilities, this can best be achieved by using services to share information and increase agility. This evolution requires that information and functional capability owners and producers begin populating the NCE with valuable net-centric services (Figure 3).

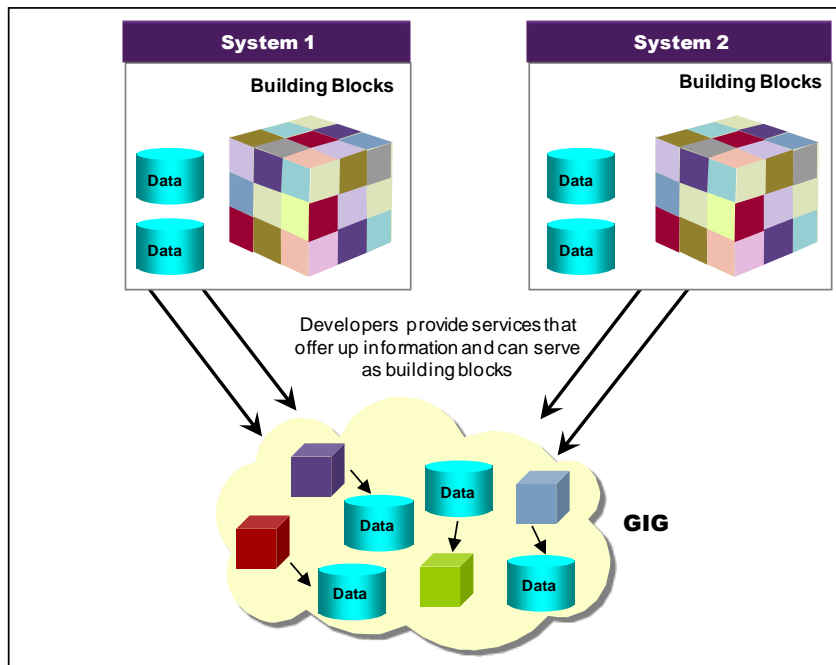


Figure 3 Populating the NCE with Services

The NCSS vision requires that program and system developers provide their information (i.e., databases in Figure 3) or functional building blocks (i.e., colored blocks in Figure 3) as services to the NCE.

Figure 4 identifies two classes of users. Warfighter and analysts will be able to find data and information by searching the NCE (e.g., through a browser-based query). Developers will be able to find services that provide a functional capability to help carry out a business or mission function and can leverage them to build or enhance capabilities. As the NCE becomes populated with services, developers will search for and use, or enhance, existing services before developing new capabilities.

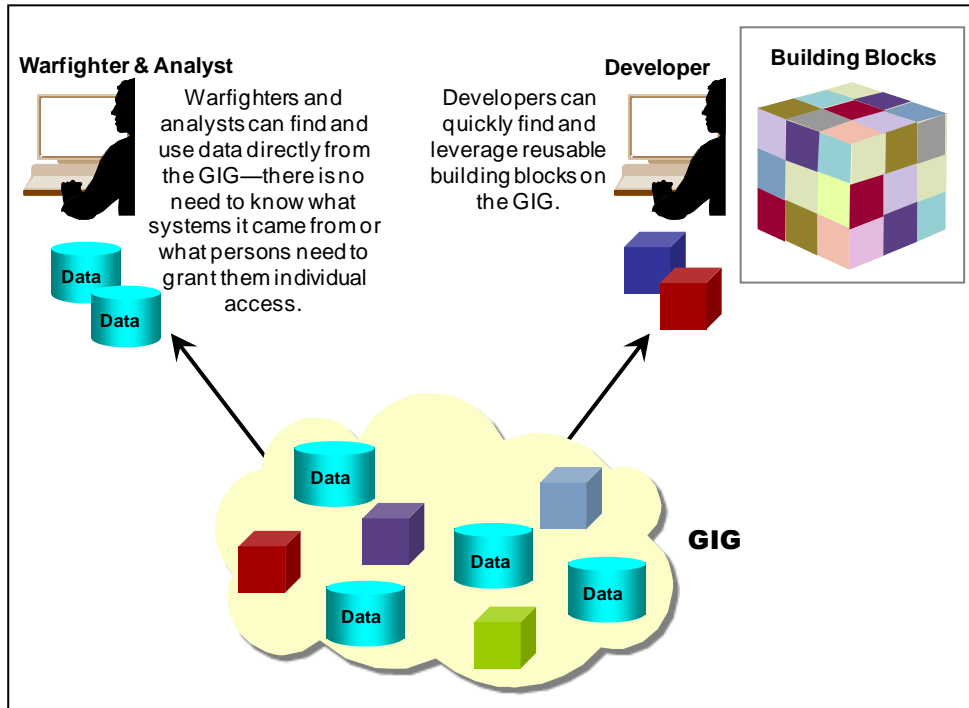


Figure 4 Users Look to the NCE for Information and Capabilities

3 Net-Centric Services Strategy Goals

To achieve the vision of establishing a DoD NCE that increasingly leverages shared services and SOA, the NCSS defines the following goals:

Table 1 Net-Centric Services Strategy Goals

Goal	Description
Provide Services	Make information and functional capabilities available as appropriately secure services on the network.
Use Services	Use existing services to satisfy mission needs before creating duplicative capabilities.
Govern the Infrastructure and Services	Establish the policies and processes for a single set of common standards, rules, and shared secure infrastructure and services throughout the DoD Enterprise to ensure interoperability.
Monitor and Manage Services via GIG NetOps	Implement services in accordance with DoD’s GIG NetOps Strategy and concept of operations to ensure situational awareness of the NCE.

These goals address how the DoD’s substantial legacy and new IT investments can evolve into an environment populated with shared services that make information and capabilities available across the enterprise.

An approach for achieving the goals of the *DoD NCSS* is presented in the following subsections.

3.1 GOAL: Provide Services

Users create services on the network to share information and to provide functional capabilities. These services are discoverable and can be accessed and used by authorized consumers in the enterprise. Services can be built or acquired in different ways, and in each case the following actions must be performed—

- Provide a description of the service and publish it to an enterprise service registry
- Build, appropriately secure, and operate the service
- Manage the performance and lifecycle of the service.

Provide Mission and Business Services

The Business, Warfighting, DoD Intelligence, and Enterprise Information Environment Mission Areas will define the mission and business processes and the specific information and functional capabilities that support them. As the NCE evolves, users will provide their information and functional capabilities to the enterprise as services. These services may be implemented by modifying and re-using existing IT systems or through new developments.

Provide Core Enterprise Services (CES)

Core Enterprise Services (CES) are a small set of services provided by the EIEMA. Some of the CES services will be centrally provided on behalf of the DoD while others might involve local provisioning. For locally provisioned services, EIEMA provides guidance to ensure consistent implementation throughout the DoD.

Make Services Visible

Providers of services must register their services in the enterprise service registry (i.e., publish the metadata describing their services) to ensure that potential users will be able to discover the

service. The enterprise-wide service registry will enable all users in the enterprise to find and understand what services already exist, thus facilitating reuse and avoiding investment in the creation of new capabilities.

Make Services Accessible

Users must not only have the ability to discover services, but must also be able to access them in a timely, secure, and effective manner. Service accessibility is controlled by security mechanisms that determine access roles and rules. Decisions on service accessibility are made and implemented by the organizations providing the service based on a variety of factors. However, service providers must use the core security services provided by the EIEMA to ensure that widest possible access is supported.

Make Services Understandable

Providers of services must use a common set of service description information to enable consistent discovery by users throughout the enterprise. A Service Specification Template (SST) will serve as the common model for providing service description information. The SST will capture, at a minimum, the following information about a service:

- What the service does
- How users can access the service
- Which security mechanisms or restrictions apply to the service
- Various points of contact for the service (e.g., the name, contact information for the service provider)
- Service-level characteristics
- Performance information.

In addition to descriptive information about services, Communities of Interest (COIs) will define the vocabularies and business rules that underlie the implementation of services. This will help ensure that the inputs and outputs for a service are well-understood and consistent within a functional community (e.g., all services that provide satellite situational awareness will use consistent terminology and rules for providing information back to users).

3.2 GOAL: Use Services

The first preference of users (i.e. warfighters, analyst/operators, developers) is to use existing services to satisfy mission needs.

Use Services as a Common Practice

Users recognize the value of information and capabilities that can be found on the network. Accordingly, existing services can be used to obtain information to support decision making processes and to execute various aspects of the warfighter and analyst missions. Developers will construct new business/mission processes by using or modifying existing services provided by Mission Areas before promoting investments in new services and systems. All users will then provide feedback (i.e., details concerning the perceived value, performance, usability) on the various services they use.

Use CES

The DoD CIO will mandate the use of some CES as they mature. Their use is mandated to enable networked joint force capabilities, improved interoperability, and increased information sharing across Mission Area services.

3.3 GOAL: Govern the Infrastructure and Services

Governance means establishing and enforcing how DoD Components and mission partners, on behalf of the Mission Areas, agree to provide, secure, use, and operate services. There are three elements to governance:

1. Identifying the attributes for providing, securing, using, and operating services that have to be governed and what level of governance is required
2. Establishing lines of responsibility, authority, and communication for making decisions about services across the lifecycle of services
3. Establishing the measurement, policy, and incentive/control mechanisms to ensure that individuals and organizations carry out their responsibilities.

Governance of a single set of common standards, rules, shared secure infrastructure, and services throughout the DoD Enterprise requires governance at various levels in the DoD. This layered approach is analogous to the approach used to govern sports leagues. In a sporting league, each team maintains its own governance (e.g., training regime, coaching, concessions, and some elements of the venue); however, when teams compete, there is a set of rules and responsibilities that all teams agree to follow (i.e., specifics of the field of play and permissible equipment to ensure a fair competition). Similarly, under the net-centric services vision, each DoD Component or program will maintain its own governance for things such as commercial middleware choices or contract management; however, when services are shared, the provisioning, securing, use, and operation will be governed in accordance with an additional set of attributes.

It is the intent of the DoD CIO to develop an enterprise governance process and to limit enterprise governance to those attributes critical to the realization of interoperable, shared services throughout the DoD and mission partners. There will be specific capabilities that require additional governance. One specific example is an enterprise capability delivered through a federation of services; in other words, a federated capability. In this strategy, a federated capability is defined as one that has the following characteristics:

- It is implemented using information sources or capabilities from a variety of service providers who are distributed across the enterprise *and*
- All service providers contributing to the federated capability agree to the definition of the service (i.e., the functionality being provided), the service interfaces, the service security properties, the semantics and structure of its payload, and the operational performance characteristics.

The additional governance required by the federation of services is defined by, agreed to, and mutually enforced by the distributed set of providers across the enterprise.

The Enterprise White Pages is a specific example of a federated capability. Each of the DoD Components and mission partners maintains an authoritative directory of users who will become part of the federation. Each member of the federation participates in defining the service

interfaces, data items, and data quality for the directory, and enforces those definitions locally. As a result of this federation, users on the GIG will be able to search for locator information on any individual in the GIG.

The DoD CIO will govern the use of federation in the DoD Enterprise services environment to ensure that the various federation management models are consistently applied and understood.

Establish Appropriate Governance Forums

Governance forums will be required at various levels across the DoD Enterprise and with mission partners. To achieve this net-centric services vision, governance will have to be implemented at the DoD Component, Mission Area, Enterprise and external partner level. The elements of governance at each of these levels will need to be defined and coordinated to ensure appropriate attention without unnecessarily limiting agility.

Enable Services to be Trusted

A range of mechanisms enables the trusted use of services from many different providers. The SST and registries provide means of delivering validated information on the identity of providers and the capability of their services to both anticipated and unanticipated consumers. Services will be published in the registry with stipulation of the specific performance and security characteristics as described in the SST. Users with appropriate and authenticated credentials will be able to use registered services under those published terms. In other cases, depending on the criticality of the mission, users of the services may need to negotiate specific performance guarantees in service level agreements (SLAs).

Integrate Service and SOA Enablers into Decision Support and Portfolio Management Processes

It is critical that the DoD's key processes support the services lifecycle in the Enterprise. This includes acquisition, testing, certification, accreditation, and portfolio management. The DoD CIO will work closely with the decision support process owners to adjust and enhance their processes to support the development of shared secure services, encourage the use of existing services, and to help guide programs and architects in developing services that are aligned with the business processes and activities necessary to carrying out their missions. Portfolio managers will continually assess the use of services and adherence to COI-defined vocabularies and business rules in executing mission and business processes. The DoD's tools and processes will be updated to support services and SOA constructs.

3.4 GOAL: Monitor and Manage Services via GIG NetOps

As services are used across the Enterprise, consumers must know if services cease to function, are no longer available, do not operate as described, or have changed. SLAs must be defined to describe the reliability and performance of services to consumers. In addition, service providers must be monitored to ensure that they are meeting SLAs. All services must be implemented in accordance with the DoD's GIG NetOps Strategy and concept of operations. Service providers must provide visibility into the real-time operational status and performance of their services against service-level agreements associated with their use.

GIG NetOps, through its federated construct, is also responsible to manage service operations to ensure the NCE is protected, that service security is not compromised, and that priorities are maintained for critical mission services.

4 Next Steps

To achieve these goals, the DoD CIO will lead four near term actions (Table 2):

Table 2 Key Actions

Key Actions	Outcome
1. Execute PDM-III Core Services Recommendations	<ul style="list-style-type: none"> • Expedite delivery of the CES that constitute the common, shared secure infrastructure of the net-centric services vision
2. Update appropriate policies and provide implementation guidance to codify use of services and SOA	<ul style="list-style-type: none"> • Establish DoD services and SOA governance through policy and guidance (e.g., DoDD 8100.1 and DoDD 8115.1; GIG Architecture Framework; Net-Centric Implementation Documents)
3. Establish a business process and model for provision and use of services	<ul style="list-style-type: none"> • Promote the funding, acquisition, creation, management, and use of services through changes to DoD decision support processes (e.g., JCIDS, DAS, PPBE, PFM)
4. Develop education and training on services and SOA	<ul style="list-style-type: none"> • Awareness and understanding of services and SOA principles will increase through the use of institutional educational resources (e.g., DAU, NDU Information Resources Management College)

The PDM-III Core Services action memorandum, signed by the Deputy Secretary of Defense in October 2006, establishes a series of actions that will expedite the delivery of the common, shared secure infrastructure. The DoD CIO has established an execution team to coordinate and assist in executing the memorandum’s action items.

During FY07 and FY08, the DoD CIO will provide additional details on DoD direction concerning service approaches. Various DoD issuances will be considered for codification of this strategy, including existing directives and instructions. Specific areas of the strategy that will be addressed include standards and guidance for using CES, governance processes for programs and COIs, identification and application of metrics and incentives, and the transition of legacy systems to accommodate service approaches.

The DoD CIO recognizes that the DoD decision support processes require change to encourage the providing, using, operating, and governing of services in the NCE. During FY07 and FY08, the DoD CIO will identify and collaborate with the process owners to implement changes that promote implementation of this strategy. These changes will be closely worked with the DoD’s emerging portfolio management processes.

Finally, the DoD CIO will establish an ongoing awareness campaign to promote the services goals for the NCE. This will include developing education and training to increase awareness of services and SOA principles, and to highlight benefits and best practices. In addition, current COI activities will be used to refine the use of services and capture best practices and lessons learned. The lessons learned will be used in the development of planning and implementation guidance.

5 Conclusion

Implementing the approach outlined in the *NCSS* will require the active participation of all DoD Components in collaboration with the DoD CIO. Maturing the NCE to one that leverages shared services and SOA requires the DoD's commitment, particularly as DoD Components migrate legacy systems. There is much work needed to establish the governance processes and to deliver the necessary CES that achieve the goals of this strategy. DoD Components will continue to evolve towards a service orientation as the broader governance forums are established and CES are implemented and deployed. In executing this strategy, the DoD CIO will continuously seek to refine the approach and maintain communications to ensure that the DoD can realize the benefits that result from achieving the vision.

6 Appendix A. Definitions

Access: to interact with a system entity to manipulate, use, gain knowledge of, and/or obtain a representation of some or all of a system entity's resources.

Agility: the ability of an organization to respond quickly to demands or opportunities.

Access Control: protection of resources against unauthorized access; a process by which the use of resources is regulated by a security policy and is permitted by only authorized system entities according to that policy.

Attribute: a distinct characteristic inherent in or ascribed to an entity; an entity's attributes are said to describe it.

Authentication: to confirm a system entity's asserted principal identity with a specified or understood level of confidence.

Authoritative: recognized by appropriate governing authorities to be valid or trusted (e.g., the United States [U.S.] Postal Service is the authoritative source for U.S. mailing ZIP codes).

Business Function: something an enterprise does, or needs to do, in order to achieve its objectives.

Business Process: the complete response that a business makes to an event. A business process entails the execution of a sequence of one or more process steps. It has a clearly defined deliverable or outcome. A business process is defined by the business event that triggers the process, the inputs and outputs, all the operational steps required to produce the output, the sequential relationship between the process steps, the business decisions that are part of the event response, and the flow of material and/or information between process steps.

Core Enterprise Services: that small set of services, whose use is mandated by the CIO, to provide awareness of, access to and delivery of information on the GIG.

Consumer: an entity (human or machine) that makes use of a service to meet a particular need.

Credential: data that is transferred to establish a claimed principal identity.

EIEMA: the Enterprise Information Environment Mission Area (EIEMA) is the DoD portfolio of programs, projects, and systems that deliver the EIE. The EIEMA portfolio enables the functions of the other mission areas, and encompasses all communications, computing, information assurance, and core enterprise service systems, equipment, or software that provide a common information capability or service for enterprise use.

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 11103 of title 40 of the United States Code. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions

(strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria: 1) transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services; 2) provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services; and 3) processes data or information for use by other equipment, software, or services.

Governance: the systems, processes, and procedures put in place to steer the direction, management, and accountability of an organization. In the context of the SOA in the DoD, governance means establishing and enforcing how DoD Components agree to provide, use, and operate services.

Identity: the collective set of attributes that defines an entity (i.e., subject, resource, etc.) within a given context.

Mission Area: a defined area of responsibility with functions and processes that contribute to mission accomplishment. In the context of managing the DoD's portfolios of GIG investments, the DoD has four major categories of mission areas - the Warfighter Mission Area, the Business Mission Area, the Defense Intelligence Mission Area, and the Enterprise Information Environment Mission Area (EIEMA).

Net-Centric Environment (NCE): the Net-Centric Environment is a framework for full human and technical connectivity and interoperability that allows all DoD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence; and protects information from those who should not have it. (Net-Centric Environment Joint Functional Concept, Version 1.0, April 7, 2005)

Service: a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description.

Service Oriented Architecture: a paradigm for defining, organizing, and utilizing distributed capabilities in the form of loosely coupled software services that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with, and use capabilities to produce desired effects that are consistent with measurable preconditions and expectations.

Service Provider: an entity (i.e., person or organization) that offers the use of capabilities by means of a service.

Workflow: a graphic representation of the flow of work in a process and its related subprocesses; including specific activities, information dependencies, and the sequence of decisions and activities.

Appendix B. References

- [1] The National Defense Strategy of the United States of America, March 2005
- [2] Department of Defense Net-Centric Data Strategy, May 9, 2003
- [3] DoD Directive 8115.01, "DoD Information Technology Portfolio Management," October 10, 2005
- [4] DoD Instruction 8115.02, "Information Technology Portfolio Management Implementation", October 30, 2006
- [5] Joint Concept of Operations for Global Information Grid NetOps, Version 3, August 4, 2006